(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2006 046 017 A1** 2008.04.03

(12) **Offenlegungsschrift**

(21) Aktenzeichen: **10 2006 046 017.0**
(22) Anmeldetag: **28.09.2006**
(43) Offenlegungstag: **03.04.2008**

(51) Int Cl.[8]: ***H04L 9/14*** (2006.01)

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Bücker, Wolfgang, 85579 Neubiberg, DE; Horn, Günther, Dr., 81541 München, DE; Thiruvengadam, Srinath, 81737 München, DE

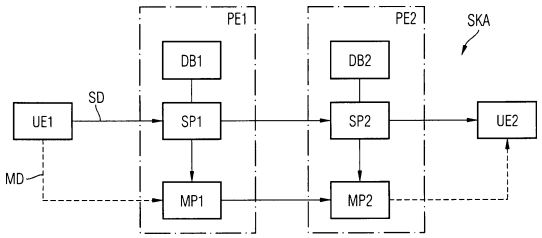
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
US2005/00 44 365 A1
WO 2004/0 75 584 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gemäß § 44 PatG ist gestellt.

(54) Bezeichnung: **Verfahren zum Bereitstellen eines symmetrischen Schlüssels zum Sichern eines Schlüssel-Management-Protokolls**

(57) Zusammenfassung: Das Verfahren zum Bereitstellen eines symmetrischen Schlüssels zum Sichern eines Schlüssel-Management-Protokolls, mittels welchem kryptographisches Material für ein Protokoll zum verschlüsselten Übertragen von Mediendaten zwischen einer Teilnehmereinrichtung und einer Provider-Einrichtung generiert wird, weist folgende Schritte auf:
Bereitstellen eines ersten symmetrischen Schlüssels der Teilnehmereinrichtung und der Provider-Einrichtung, welcher in einem auf symmetrischen Schlüsseln basierenden Sicherungsmechanismus eines Netzprotokolls einer Kontrollschicht zum Aufbau einer Kommunikationssitzung zwischen der Teilnehmereinrichtung und der Provider-Einrichtung eingesetzt wird; Bereitstellen eines ersten zeitveränderlichen Parameters durch die Provider-Einrichtung; Übertragen des bereitgestellten ersten zeitveränderlichen Parameters von der Provider-Einrichtung an die Teilnehmereinrichtung; Berechnen eines zweiten symmetrischen Schlüssels für das Sichern des Schlüssel-Management-Protokolls mittels einer vorbestimmten Funktion in Abhängigkeit zumindest des bereitgestellten ersten symmetrischen Schlüssels und des bereitgestellten ersten zeitveränderlichen Parameters durch die Provider-Einrichtung und Berechnen des zweiten symmetrischen Schlüssels mittels der vorbestimmten Funktion in Abhängigkeit zumindest des bereitgestellten ersten symmetrischen Schlüssels und des übertragenen ersten zeitveränderlichen Parameters duch die Teilnehmereinrichtung.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Bereitstellen eines symmetrischen Schlüssels zum Sichern eines Schlüssel-Management-Protokolls.

[0002] Das technische Gebiet der vorliegenden Erfindung betrifft das Sichern oder Verschlüsseln von Mediendaten zwischen einer Teilnehmereinrichtung, wie einem Personal-Computer, und einer Provider-Einrichtung, beispielsweise einem Medien-Server eines Dienstleisters oder Providers.

[0003] In den heutigen im Einsatz befindlichen SIP/RTP basierten Voice-over-IP Systemen (wie z.B. dem IP Multimedia Subsystem – IMS) werden typischerweise keine Maßnahmen zum Schutz der Mediendaten ergriffen. Dies mag vertretbar sein in Mobilfunknetzen, die typischerweise eine Layer 2 Verschlüsselung anbieten, wie z.B. das UMTS bzw. GPRS Netz. In Festnetz-Szenarien sind aber solche unterliegenden Layer 2 Verschlüsselungen typischerweise nicht vorhanden, so dass hier eigene Mechanismen eingesetzt werden müssen. Dies ist umso dringlicher, als beispielsweise das IMS in zunehmendem Maße auch in Festnetz-Szenarien eingesetzt wird und nicht nur im Mobilnetz-Umfeld, wofür es ursprünglich entwickelt wurde.

[0004] Ein möglicher Ansatz zum Sichern der Mediendaten besteht in einer Ende-zu-Ende Verschlüsselung zwischen den beiden Kommunikationspartnern. Hier trifft man allerdings auf diverse Probleme wie z.B. Schlüssel-Management, Lawful Interception, Transcodierung etc. Eine bessere Variante scheint daher ein Ende-zu-Mitte (end-to-middle) Ansatz zu sein, bei dem die Sicherung nur zwischen dem Endgerät und einer Providereinrichtung (z.B. einem Medien-Proxy) erfolgt.

[0005] In einem Ende-zu-Ende-Sicherheitsszenario sind die Signalisierungsendpunkte und die Mediensicherheitsendpunkte dieselben, in einem Ende-zu-Mitte-Szenario sind sie verschieden. RFC 3711 definiert ein Profil für RTP, nämlich Secure-RTP (SRTP), um den RTP-Strom zu sichern. SRTP kann genutzt werden, um den Medienverkehr bei einer End-zu-End-Verbindung zu sichern, d.h. den kompletten Pfad zwischen zwei kommunizierenden Teilnehmern. Auch für eine Ende-zu-Mitte-Verbindung ist RTP einsetzbar.

[0006] Es ist eine Aufgabe der vorliegenden Erfindung, Mediendaten zwischen einer Teilnehmereinrichtung und einer Provider-Einrichtung hinsichtlich Integrität und Vertraulichkeit unter Verwendung eines geeigneten Sicherheitsprotokolls, wie SRTP, zu schützen.

[0007] Allerdings muss ein solches Sicherheitsprotokoll mit einem geeigneten Hauptschlüssel zur Ableitung von Sitzungsschlüsseln und kryptographischem Kontext ausgestattet werden. Ein Beispiel für einen kryptographischen Kontext ist in Abschnitt 3.2 des RFC 3711 beschrieben. Vor dem Start einer Kommunikation zwischen der Teilnehmereinrichtung und der Provider-Einrichtung, wie beispielsweise einem Medien-Proxy, sind der Hauptschlüssel und der kryptographische Kontext nicht in der Teilnehmereinrichtung und der Provider-Einrichtung verfügbar. Somit ist es notwendig, Mittel vorzusehen, welche den Hauptschlüssel und den kryptographischen Kontext bereitstellen. Für diesen Zweck kann ein Schlüssel-Management-Protokoll eingesetzt werden. Ein Beispiel für ein Schlüssel-Management-Protokoll für SRTP ist MIKEY. MIKEY ist beschrieben in RRC 3830. Das Schlüssel-Management-Protokoll wird zwischen der Teilnehmereinrichtung und dem geeigneten Server des Netzwerkes ausgeführt. Der geeignete Server muss nicht der Medien-Proxy sein. Alternativ kann dieser auch mit dem SIP-Proxy zusammenfallen. Allerdings muss das Schlüssel-Management-Protokoll selbst gesichert werden.

[0008] Somit ist eine weitere Aufgabe der vorliegenden Erfindung, ein Schlüssel-Management-Protokoll für ein Protokoll zum verschlüsselten Übertragen von Mediendaten, wie SRTP, zwischen einer Teilnehmereinrichtung und einer Provider-Einrichtung zu sichern.

[0009] Des Weiteren ist es eine Aufgabe, symmetrische Schlüssel einer Teilnehmereinrichtung und einer entsprechenden Provider-Einrichtung zum Sichern eines Schlüssel-Management-Protokolls für ein Protokoll zum verschlüsselten Übertragen von Mediendaten zwischen der Teilnehmereinrichtung und der Provider-Einrichtung bereitzustellen.

[0010] Erfindungsgemäß wird zumindest eine dieser gestellten Aufgabe durch ein Verfahren mit den Merkmalen des Patentanspruchs 1 und/oder durch ein Verfahren mit den Merkmalen des Patentanspruchs 15 gelöst.

[0011] Demgemäß wird ein Verfahren zum Bereistellen eines symmetrischen Schlüssels zum Sichern eines Schlüssel-Management-Protokolls vorgeschlagen, mittels welchem kryptographisches Material für ein Protokoll zum verschlüsselten Übertragen von Mediendaten zwischen einer Teilnehmereinrichtung und einer Provider-Einrichtung generiert wird, wobei das Verfahren folgende Schritte aufweist:

– Bereitstellen eines ersten symmetrischen Schlüssels der Teilnehmereinrichtung und der Provider-Einrichtung, welcher in einem auf symmetrischen Schlüsseln basierenden Sicherungsmechanismus eines Netzprotokolls einer Kontrollschicht zum Aufbau einer Kommunikationssitzung zwischen der Teilnehmereinrichtung und der Pro-

vider-Einrichtung eingesetzt wird;
– Bereitstellen eines ersten zeitveränderlichen Parameters durch die Provider-Einrichtung;
– Übertragen des bereitgestellten ersten zeitveränderlichen Parameters von der Provider-Einrichtung an die Teilnehmereinrichtung;
– Berechnen eines zweiten symmetrischen Schlüssels für das Sichern des Schlüssel-Management-Protokolls mittels einer vorbestimmten Funktion in Abhängigkeit zumindest des bereitgestellten ersten symmetrischen Schlüssels und des bereitgestellten ersten zeitveränderlichen Parameters durch die Provider-Einrichtung; und
– Berechnen des zweiten symmetrischen Schlüssels mittels der vorbestimmten Funktion in Abhängigkeit zumindest des bereitgestellten ersten symmetrischen Schlüssels und des übertragenen ersten zeitveränderlichen Parameters durch die Teilnehmereinrichtung.

[0012] Des Weiteren wird ein Verfahren zum Verschlüsseln von Mediendaten zwischen einer Teilnehmereinrichtung und einer Provider-Einrichtung vorgeschlagen, welches folgende Schritte aufweist:
– Bereitstellen eines symmetrischen Schlüssels jeweils der Teilnehmereinrichtung und der Provider-Einrichtung mittels des oben erläuterten Verfahrens zum Bereitstellen eines symmetrischen Schlüssels zum Sichern eines Schlüssel-Management-Protokolls;
– Verschlüsseln der Mediendaten in Abhängigkeit des symmetrischen Schlüssels durch die Teilnehmereinrichtung oder die Provider-Einrichtung;
– Senden der verschlüsselten Mediendaten durch die Teilnehmereinrichtung oder die Provider-Einrichtung;
– Empfangen der verschlüsselten Mediendaten durch die Provider-Einrichtung oder die Teilnehmereinrichtung; und
– Entschlüsseln der empfangenen Mediendaten mittels des bereitgestellten symmetrischen Schlüssels durch die Provider-Einrichtung oder die Teilnehmereinrichtung.

[0013] Vorteilhafterweise stellt die vorliegenden Erfindung eine Möglichkeit bereit, das Schlüssel-Management-Protokoll, mittels welchem kryptographisches Material für ein Protokoll, wie SRTP, zum verschlüsselten Übertragen von Mediendaten zwischen einer Teilnehmereinrichtung und einer Provider-Einrichtung generiert wird, zu sichern. Die Sicherung des Schlüssel-Management-Protokolls wird vorteilhafterweise durch ein einfach handhabbares, symmetrisches Verschlüsselungsverfahren mit einem symmetrischen Schlüssel gesichert.

[0014] Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen sowie der Beschreibung der Bezugnahme auf die Zeichnungen.

[0015] Gemäß einer bevorzugten Ausgestaltung der Erfindung ist das Protokoll zum verschlüsselten Übertragen der Mediendaten als Secure-Real-Time-Transport-Protokoll (SRTP) ausgebildet.

[0016] Gemäß einer weiteren bevorzugten Ausgestaltung ist das Schlüssel-Management-Protokoll als Multimedia-Internet-Keying (MIKEY) ausgebildet.

[0017] Gemäß einer weiteren bevorzugten Ausgestaltung ist der Sicherungsmechanismus als Authentifizierungs- und/oder Integritätsprotokoll, insbesondere als HTTP-Digest-Protokoll, ausgebildet.

[0018] Gemäß einer weiteren bevorzugten Ausgestaltung ist das Netzprotokoll zum Aufbau der Kommunikationsverbindung als Session-Initiation-Protokoll (SIP) ausgebildet.

[0019] Gemäß einer weiteren bevorzugten Ausgestaltung weist das kryptographische Material einen Hauptschlüssel zur Ableitung von Sitzungsschlüsseln und kryptographischen Kontext auf.

[0020] Gemäß einer weiteren bevorzugten Ausgestaltung wird das Schlüssel-Management-Protokoll in der Kontrollschicht und/oder in einer Medienschicht eingesetzt.

[0021] Gemäß einer bevorzugten Weiterbildung der Erfindung weist das oben erläuterte Verfahren weiter folgende Schritte auf:
– Generieren eins zweiten zeitveränderlichen Parameters durch die Teilnehmereinrichtung;
– Übertragen des generierten zweiten zeitveränderlichen Parameters von der Teilnehmereinrichtung an die Provider-Einrichtung;
– Berechnen des zweiten symmetrischen Schlüssels in Abhängigkeit des bereitgestellten ersten symmetrischen Schlüssels, des bereitgestellten ersten zeitveränderlichen Parameters und des von der Teilnehmereinrichtung übertragenen, zweiten zeitveränderlichen Parameters durch die Provider-Einrichtung; und
– Berechnen des zweiten symmetrischen Schlüssels in Abhängigkeit des bereitgestellten ersten symmetrischen Schlüssels, des von der Provider-Einrichtung übertragenen ersten zeitveränderlichen Parameters und des generierten zweiten zeitveränderlichen Parameters durch die Teilnehmereinrichtung.

[0022] Gemäß einer weiteren bevorzugten Weiterbildung wird ein dritter zeitveränderlicher Parameter jeweils durch die Teilnehmereinrichtung und die Provider-Einrichtung von dem ersten zeitveränderlichen Parameter abgeleitet, in dessen Abhängigkeit der zweite symmetrische Schlüssel jeweils durch die Teilnehmereinrichtung und die Provider-Einrichtung berechnet wird.

[0023] Gemäß einer weiteren bevorzugten Ausgestaltung ist der erste zeitveränderliche Parameter als eine Number-Used-Once (Nonce) und/oder der zweite zeitveränderliche Parameter als eine Client-Defined-Nonce (CNonce) und/oder der dritte zeitveränderliche Parameter als ein Nonce-Count des HTTP-Digest-Protokolls ausgebildet.

[0024] Gemäß einer weiteren bevorzugten Ausgestaltung ist die vorbestimmte Funktion in eine erste Teil-Funktion und in eine zweite Teil-Funktion teilbar, wobei die erste Teil-Funktion zumindest den ersten symmetrischen Schlüssel und den ersten zeitveränderlichen Parameter als Eingangsparameter hat und die zweite Teil-Funktion zumindest ein Ergebnis der ersten Teil-Funktion und den zweien zeitveränderlichen Parameter als Eingangsparameter hat.

[0025] Gemäß einer weiteren bevorzugten Ausgestaltung bilden die Teilnehmereinrichtung und die Provider-Einrichtung zumindest teilweise ein IP-Multimedia-Subsystem (IMS) aus.

[0026] Gemäß einer weiteren bevorzugten Ausgestaltung weist die Provider-Einrichtung des IP-Multimedia-Subsystems (IMS) auf:

– eine Proxy-Funktionalitätseinheit, welche mit der Teilnehmereinrichtung gekoppelt ist, und/oder
– eine Interrogations-Funktionalitätseinheit, welche mit der Proxy-Funktionalitätseinheit gekoppelt ist, und/oder
– eine Server-Funktionalitätseinheit, welche mit der Interrogations-Funktionalitätseinheit gekoppelt ist, und/oder
– eine Home-Subscriber-Server-Einheit, welche mit der Server-Funktionalitätseinheit gekoppelt ist und zumindest den ersten symmetrischen Schlüssel speichert.

[0027] Gemäß einer weiteren bevorzugten Ausgestaltung wird das HTTP-Digest-Protokoll zwischen der Teilnehmereinrichtung und der Server-Funktionalitätseinheit ausgeführt.

[0028] Gemäß einer weiteren bevorzugten Ausgestaltung wird das HTTP-Digest-Protokoll zwischen der Teilnehmereinrichtung und der Home-Subscriber-Server-Einheit ausgeführt.

[0029] Gemäß einer weiteren bevorzugten Ausgestaltung wird die erste Teil-Funktion von der Server-Funktionalitätseinheit ausgeführt, das Ergebnis der ersten Teil-Funktion wird von der Server-Funktionalitätseinheit an die Proxy-Funktionalitätseinheit übertragen, der zweite zeitveränderliche Parameter wird von der Proxy-Funktionalitätseinheit empfangen und die zweite Teil-Funktion wird von der Proxy-Funktionalitätseinheit ausgeführt.

[0030] Gemäß einer weiteren bevorzugten Ausgestaltung wird die erste Teil-Funktion von der Home-Subscriber-Server-Einheit ausgeführt, das Ergebnis der ersten Teil-Funktion wird von der Home-Subscriber-Server-Einheit an die Proxy-Funktionalitätseinheit über die Interrogations-Funktionalitätseinheit übertragen, der zweite zeitveränderliche Parameter wird von der Proxy-Funktionalitätseinheit empfangen und die zweite Teil-Funktion wird von der Proxy-Funktionalitätseinheit ausgeführt.

[0031] Gemäß einer weiteren bevorzugten Ausgestaltung hat die Teilnehmereinrichtung eine SIP-basierte Subskription mit der Provider-Einrichtung.

[0032] Die Erfindung wird nachfolgend anhand der in den schematischen Figuren angegebenen Ausführungsbeispiele näher erläutert. Es zeigen:

[0033] Fig. 1 ein schematisches Blockschaltbild einer SIP-basierten Kommunikations-Architektur, auf welches das erfindungsgemäße Verfahren anwendbar ist;

[0034] Fig. 2 ein schematisches Ablaufdiagramm eines ersten Ausführungsbeispiels des erfindungsgemäßen Verfahrens;

[0035] Fig. 3 ein schematisches Ablaufdiagramm eines zweiten Ausführungsbeispiels des erfindungsgemäßen Verfahrens;

[0036] Fig. 4 ein schematisches Blockschaltbild einer IMS-Architektur, auf welche das erfindungsgemäße Verfahren anwendbar ist;

[0037] Fig. 5 ein schematisches Ablaufdiagramm eines dritten, auf die IMS-Architektur gemäß Fig. 4 angewendeten Ausführungsbeispiels des erfindungsgemäßen Verfahrens; und

[0038] Fig. 6 ein schematisches Ablaufdiagramm eines vierten, auf die IMS-Architektur gemäß Fig. 4 angewendeten Ausführungsbeispiels des erfindungsgemäßen Verfahrens.

[0039] In allen Figuren sind gleiche bzw. funktionsgleiche Elemente und Einheiten – sofern nichts anderes angegeben ist – mit denselben Bezugszeichen versehen worden.

[0040] Fig. 1 zeigt ein schematisches Blockschaltbild einer SIP-basierten Kommunikations-Architektur SKA, auf welche das erfindungsgemäße Verfahren anwendbar ist.

[0041] Die SIP-basierte Kommunikations-Architektur SKA gemäß Fig. 1 ist durch eine erste Teilnehmereinrichtung UE1, eine erste Provider-Einrichtung PE1, eine zweite Provider-Einrichtung PE2 und eine zweite Teilnehmereinrichtung UE2 ausgebildet. Da-

bei ist die erste Teilnehmereinrichtung UE1 mit der ersten Provider-Einrichtung PE1 gekoppelt. Die zweite Teilnehmereinrichtung UE2 ist mit der zweiten Provider-Einrichtung PE2 gekoppelt. Weiterhin sind die erste Provider-Einrichtung PE1 und die zweite Provider-Einrichtung PE2 gekoppelt. Die Koppelung zwischen der ersten Provider-Einrichtung PE1 und der zweiten Provider-Einrichtung PE2 kann durch ein Netzwerk, insbesondere dem Internet, ausgebildet sein.

[0042] Eine Provider-Einrichtung PE1, PE2 weist eine Datenbank DB1, DB2, eine SIP-Proxy-Funktionalitätseinheit SP1, SP2 und eine Media-Proxy-Funktionalitätseinheit MP1, MP2 auf.

[0043] Das Session-Initiation-Protokoll SIP wird insbesondere zwischen der Teilnehmereinrichtung UE1 und der SIP-Funktionalitätseinheit SP1 ausgeführt. Aus Gründen der Übersichtlichkeit ist eine entsprechende Darstellung für die zweite Teilnehmereinrichtung UE2 und die zweite Provider-Einrichtung PE2 nicht dargestellt.

[0044] Das Secure-Real-Time-Protokoll SRTP wird zwischen der ersten Teilnehmereinrichtung UE1 und der Media-Proxy-Funktionalitätseinheit MP1 ausgeführt.

[0045] In Fig. 2 ist ein schematisches Ablaufdiagramm eines ersten Ausführungsbeispiels des erfindungsgemäßen Verfahrens zum Bereitstellen eines symmetrischen Schlüssels NK zum Sichern eines Schlüssel-Management-Protokolls, mit welchem krytographisches Material für ein Protokoll zum verschlüsselten Übertragen von Mediendaten MD zwischen der Teilnehmereinrichtung UE1 und der Provider-Einrichtung PE1 generiert wird, dargestellt. Nachfolgend wird das erfindungsgemäße Verfahren anhand des Blockschaltbildes in Fig. 2 unter Verweis auf die Architektur gemäß Fig. 1 beschrieben. Das erste Ausführungsbeispiel des erfindungsgemäßen Verfahrens gemäß Fig. 2 weist folgende Verfahrensschritte S1 bis S5 auf:

Verfahrensschritt S1:

[0046] Ein erster symmetrischer Schlüssel DK wird der Teilnehmereinrichtung UE1 und der Provider-Einrichtung PE1 bereitgestellt. Der erste symmetrische Schlüssel DK wird in einem auf symmetrischen Schlüsseln basierenden Sicherungsmechanimus eines Netzprotokolls einer Kontrollschicht zum Aufbau einer Kommunikationssitzung zwischen der Teilnehmereinrichtung UE1 und der Provider-Einrichtung PE1 eingesetzt.

Verfahrensschritt S2:

[0047] Es wird ein erster zeitveränderlicher Parameter Nonce durch die Provider-Einrichtung PE1 bereitgestellt.

Verfahrensschritt S3:

[0048] Der bereitgestellte erste zeitveränderliche Parameter Nonce wird von der Provider-Vorrichtung PE1 an die Teilnehmereinrichtung UE1 übertragen.

Verfahrensschritt S4:

[0049] Ein zweiter symmetrischer Schlüssel NK wird für das Sichern des Schlüssel-Management-Protokolls mittels einer vorbestimmten Funktion F in Abhängigkeit zumindest des bereitgestellten ersten symmetrischen Schlüssels DK und des bereitgestellten ersten zeitveränderlichen Parameters Nonce durch die Provider-Einrichtung PE1 berechnet (NK = F(DK, Nonce)).

Verfahrensschritt S5:

[0050] Der zweite symmetrische Schlüssel NK wird mittels der vorbestimmten Funktion F in Abhängigkeit zumindest des bereitgestellten ersten symmetrischen Schlüssel DK und des übertragenen ersten zeitveränderlichen Parameters Nonce durch die Teilnehmereinrichtung UE1 berechnet (NK = F(DK, Nonce)).

[0051] Die Verfahrensschritte S4 und S5 können auch in umgekehrter Reihenfolge durchgeführt werden. Vorzugsweise wird die Provider-Einrichtung PE1 den Schlüssel NK erst berechnen, wenn die Teilnehmereinrichtung UE1 authentifiziert ist.

[0052] Somit ist sowohl der Provider-Einrichtung PE1 als auch der Teilnehmereinrichtung UE1 der symmetrische Schlüssel NK bekannt.

[0053] Ein zweites Ausführungsbeispiel des erfindungsgemäßen Verfahrens ist in Fig. 3 dargestellt. Das zweite Ausführungsbeispiel gemäß Fig. 3 weist die Verfahrensschritte T1 bis T7 auf. Dabei entsprechen die Verfahrensschritte T1 bis T3 gemäß Fig. 3 den Verfahrensschritten S1 bis S3 gemäß Fig. 2. Aus Gründen der Übersichtlichkeit wird auf deren erneute Darstellung verzichtet. Das zweite Ausführungsbeispiel gemäß Fig. 3 weist also die Verfahrensschritte T1 bis T3, welche den Verfahrensschritten S1 bis S3 gemäß Fig. 2 entsprechen, und die folgenden Verfahrensschritte T4 bis T7 auf:

Verfahrensschritt T4:

[0054] Es wird ein zweiter zeitveränderlicher Parameter CNonce durch die Teilnehmereinrichtung UE1 generiert.

Verfahrensschritt T5:

[0055] Der generierte zweite zeitveränderliche Parameter CNonce wird von der Teilnehmereinrichtung UE1 an die Provider-Einrichtung PE1 übertragen.

Verfahrensschritt T6:

[0056] Der zweite symmetrische Schlüssel NK wird in Abhängigkeit des bereitgestellten ersten symmetrischen Schlüssels DK, des bereitgestellten ersten zeitveränderlichen Parameters Nonce und des von der Teilnehmereinrichtung UE1 übertragenen, zweiten zeitveränderlichen Parameters CNonce durch die Provider-Einrichtung PE1 berechnet (NK = F(DK, Nonce, CNonce)).

Verfahrensschritt T7:

[0057] Der zweite symmetrische Schlüssel NK wird in Abhängigkeit des bereitgestellten ersten symmetrischen Schlüssels DK, des von der Provider-Einrichtung PE1 übertragenen, ersten zeitveränderlichen Parameters Nonce und des generierten, zweiten zeitveränderlichen Parameters CNonce durch die Teilnehmereinrichtung UE1 berechnet (NK = F (DK, Nonce, CNonce)).

[0058] Die Verfahrensschritte T6 und T7 können auch in umgekehrter Reihenfolge durchgeführt werden. Vorzugsweise wird die Provider-Einrichtung PE1 den Schlüssel NK erst berechnen, wenn die Teilnehmereinrichtung UE1 authentifiziert ist. Für das erfindungsgemäße Verfahren, dabei insbesondere für die Ausführungsbeispiele gemäß der Fig. 2 und Fig. 3, sind folgende Ausgestaltungen vorteilhafterweise möglich.

[0059] Das Protokoll zum verschlüsselten Übertragen der Mediendaten MD kann als Secure-Real-Time-Transport-Protokoll (SRTP) ausgebildet sein. Das Schlüssel-Management-Protokoll kann als Multimedia-Internet-Keying (MIKEY) ausgebildet sein. Der Sicherungsmechanismus kann ein Authentifizierungs- und/oder Integritätsprotokoll, dabei insbesondere ein HTTP-Digest-Protokoll sein. Das Netzwerkprotokoll zum Aufbau der Kommunikationsverbindung kann das Session-Initiation-Protokoll (SIP) sein. Weiterhin kann das kryptographische Material einen Hauptschlüssel zur Ableitung von Sitzungsschlüsseln und kryptographischem Kontext aufweisen.

[0060] Vorzugsweise wird das Schlüssel-Management-Protokoll in der Kontrollschicht und/oder in einer Medienschicht eingesetzt. Insbesondere kann auch ein dritter zeitveränderlicher Parameter Nonce-Count jeweils durch die Teilnehmereinrichtung UE1 und die Provider-Einrichtung PE1 von dem ersten zeitveränderlichen Parameter Nonce abgeleitet werden. In Abhängigkeit von diesem dritten zeitveränderlichen Parameter Nonce-Count kann der zweite symmetrische Schlüssel NK jeweils durch die Teilnehmereinrichtung UE1 und die Provider-Einrichtung PE1 berechnet werden. Insbesondere ist die HTTP-Digest-Authentification, welche erfindungsgemäß vorzugsweise als Sicherungsmechanismus eingesetzt wird, in RFC 2618 und RFC 3261 beschrieben. Vorzugsweise ist der erste zeitveränderliche Parameter als eine Number-Used-Once (Nonce) ausgebildet. Der zweite zeitveränderliche Parameter ist insbesondere eine Client-Defined-Nonce (CNonce). Der dritte zeitveränderliche Parameter ist vorzugsweise als Nonce-Count des HTTP-Digest-Protokolls ausgebildet.

[0061] Im Folgenden wird der Einsatz der Erfindung in einer IMS-Architektur erläutert. Dazu ist in Fig. 4 ein schematisches Blockschaltbild einer solchen IMS-Architektur IMS dargestellt. Das HTTP-Digest-Protokoll wird dabei als Sicherungsmechanismus für das Session-Initiation-Protokoll SIP eingesetzt. Beispiele für HTTP-Digest als Authentifizierungsmechanismus finden sich in Push-To-Talk-over-Cellular (PoC) [OMA PoC Release 1] oder in ETSI TISPAN Spezifikation ETSI TS 183033. Ein weiteres Beispiel der Verwendung von HTTP-Digest für eine IMS-Architektur ist die Packet-Cable-Spezifikation PKT-SP-33.203.

[0062] Die Provider-Einrichtung PE1 des IP-Multimedia-Subsystems IMS gemäß Fig. 4 weist eine Proxy-Funktionalitätseinheit P-CSCF, eine Interogations-Funktionseinheit I-CSCF, eine Server-Funktionalitätseinheit S-CSCF und eine Home-Subscriber-Server-Einheit HSS auf. Die Proxy-Funktionalitätseinheit P-CSCF ist mit der Teilnehmereinrichtung UE1 gekoppelt. Die Interrogations-Funktionalitätseinheit I-CSCF ist mit der Proxy-Funktionaltitätseinheit P-CSCF gekoppelt, die Server-Funktionalitätseinheit S-CSCF ist mit der Interrogations-Funktionalitätseinheit I-CSCF gekoppelt und die Home-Subscriber-Server-Einheit HSS ist mit der Server-Funktionalitätseinheit S-CSCF gekoppelt. Des Weiteren speichert die Home-Subscriber-Server-Einheit vorzugsweise den ersten symmetrischen Schlüssel DK.

[0063] Wenn also HTTP-Digest in der IMS-Architektur IMS verwendet wird, so sind die Teilnehmereinrichtung UE1 und die Home-Subscriber-Server-Einheit HSS jeweils mit dem symmetrischen Schlüssel DK für die Authentifizierung durch das HTTP-Digest ausgestattet. Während einer Sitzungs-Initiierung sendet die Teilnehmereinrichtung UE1 eine erste unauthorisierte SIP-Register-Nachricht zur P-CSCF, welche diese an die S-CSCF weiterleitet. Die S-CSCF fragt bei der HSS eine Nutzeridentifizierung oder Subscriptionsdaten ab. Dabei sind zwei Alternativen möglich:

Alternative 1:

[0064] Die S-CSCF erhält den Schlüssel DK von der HSS. Die S-CSCF speichert den Schlüssel DK zur Authentifizierung der Teilnehmereinrichtung UE1 mittels der nächsten Register-Nachricht. Die S-CSCF terminiert das HTTP-Digest-Protokoll.

Alternative 2:

[0065] Die HSS sendet den Schlüssel DK nicht an die S-CSCF. Die HSS terminiert das HTTP-Digest-Protokoll selbst und berechnet alle für das verwendete Protokoll erforderlichen Nachrichten.

[0066] Folgende zwei Beispiele zeigen zwei unterschiedliche Ausgestaltungen der Erfindung für beide oben erläuterten Alternativen:

Beispiel 1: Verwendung von Nonce ohne CNonce

Für Alternative 1:

[0067] Die S-CSCF generiert den zweiten Schlüssel NK unter Verwendung des ersten Schlüssels DK und des ersten zeitveränderlichen Parameters Nonce und sendet den zweiten Schlüssel NK in der SIP-401-Unauthorized-Nachricht zur P-CSCF. Die Teilnehmereinrichtung UE1 generiert, nachdem sie diese Nachricht empfangen hat, ebenfalls den zweiten Schlüssel NK in ähnlicher Weise unter Verwendung des ersten Schlüssels DK und des zeitveränderlichen Parameters Nonce. Allerdings hat die P-CSCF den Schlüssel NK aus der Nachricht entfernt, sonst wäre er auf dem Weg von der P-CSCF zur Teilnehmereinrichtung UE1 leicht abzuhören. Somit sind der Teilnehmereinrichtung UE1 und der P-CSCF der zweite Schlüssel NK bekannt.

Für Alternative 2:

[0068] Die HSS generiert den zweiten Schlüssel NK unter Verwendung des ersten Schlüssels DK und des ersten zeitveränderlichen Parameters Nonce mittels der vorbestimmten Funktion F und sendet den generierten zweiten Schlüssel NK in einer IMS-Nachricht zur S-CSCF, welche den zweiten Schlüssel NK in einer SIP-401-Unauthorized-Nachricht zur P-CSCF weiterleitet. Die Teilnehmereinrichtung UE1 wird ebenfalls, nachdem sie diese Nachricht empfangen hat, den zweiten Schlüssel NK in gleicher Weise unter Verwendung der Nonce und des ersten Schlüssels DK generieren. Allerdings hat die P-CSCF den Schlüssel NK aus der Nachricht entfernt, sonst wäre er auf dem Weg von der P-CSCF zur Teilnehmereinrichtung UE1 leicht abzuhören. Somit sind der ersten Teilnehmereinrichtung UE1 und der P-CSCF der zweite Schlüssel NK bereitgestellt.

Beispiel 2: Verwendung von Nonce und CNonce

Für Alternative 1:

[0069] Die S-CSCF generiert NK unter Verwendung von DK, Nonce und CNonce als Eingangsparameter für die vorbestimmte Funktion F. Aber NK kann nicht in der 401-Nachricht von der S-CSCF an die P-CSCF gesendet werden, da CNonce zu diesem Zeitpunkt in der S-CSCF nicht verfügbar ist. Allerdings ist es möglich, NK in der SIP-200-OK-Nachricht (siehe Nachricht 9 in **Fig. 5**) zu senden. Die Teilnehmereinrichtung UE1 kann ebenfalls NK mittels der vorbestimmten Funktion F unter Verwendung von DK, Nonce und CNonce generieren. Allerdings hat die P-CSCF den Schlüssel NK aus der Nachricht entfernt, sonst wäre er auf dem Weg von der P-CSCF zur Teilnehmereinrichtung UE1 leicht abzuhören. Somit besitzen die Teilnehmereinrichtung UE1 und die P-CSCF den zweiten Schlüssel NK.

[0070] Vorzugsweise kann die vorbestimmte Funktion F in eine erste Teil-Funktion F1 und eine zweite Teil-Funktion F2 unterteilt werden. Dabei hat die erste Teil-Funktion F1 zumindest den ersten symmetrischen Schlüssel DK und den ersten zeitveränderlichen Parameter Nonce als Eingangsparameter und die zweite Teil-Funktion F2 hat zumindest ein Ergebnis der ersten Teil-Funktion F1 (DK, Nonce) und den zweiten zeitveränderlichen Parameter CNonce als Eingangsparameter. Dann kann das Ergebnis der ersten Teil-Funktion (DK, Nonce) von der S-CSCF zu der P-CSCF [in der 401-Nachricht] gesendet werden und die P-CSCF kann NK in Abhängigkeit von diesem und einem abgefangenen CNonce berechnen. Dies ist dann möglich, wenn die P-CSCF die HTTP-Digest-Header empfängt oder abfängt.

Für Alternative 2:

[0071] HSS führt die erste Teil-Funktion F1 aus und berechnet deren Ergebnis F1(Nonce, DK) und sendet das Ergebnis F1(Nonce, DK) in einer IMS-Nachricht an die S-CSCF. Die S-CSCF kann dann den zweiten Schlüssel NK (NK = F2 (CNonce, F1 (Nonce, DK))) in der SIP-200-OK-Nachricht zur P-CSCF weiterleiten. Die Teilnehmereinrichtung UE1 kann dann ebenfalls, nachdem sie diese Nachricht empfangen hat, den zweiten Schlüssel NK unter Verwendung von Nonce und DK generieren. Allerdings hat die P-CSCF den Schlüssel NK aus der Nachricht entfernt, sonst wäre er auf dem Weg von der P-CSCF zur Teilnehmereinrichtung UE1 leicht abzuhören. Somit werden sowohl die Teilnehmereinrichtung UE1 als auch die P-CSCF denselben zweiten Schlüssel NK besitzen.

[0072] Als eine Variante wird das Ergebnis der ersten Teil-Funktion F1(Nonce, DK) von der S-CSCF zu der P-CSCF in der 401-Nachricht gesendet und die

P-CSCF kann den zweiten Schlüssel NK in Abhängigkeit von diesem und dem abgefangenen CNonce berechnen.

[0073] Dazu zeigt Fig. 5 ein schematisches Ablaufdiagramm des erfindungsgemäßen Verfahrens gemäß Beispiel 1 mit Alternative 1:

1. Die Teilnehmereinrichtung UE1 sendet die initiale SIP-Register-Anfrage zur Adresse der P-CSCF, welche in der IMS-Architektur IMS vorkonfiguriert ist. Die Anfrage beinhaltet einen Authorisierungs-Header, der die Private-User-Identity IMPI aufweist.
2. Die P-CSCF leitet die empfangene Nachricht zur S-CSCF über die I-CSCF weiter. Aus Gründen der Übersichtlichkeit ist die I-CSCF in den Fig. 5 und Fig. 6 nicht dargestellt.
3. Nachdem die SIP-Register-Anfrage empfangen wurde, überträgt die S-CSCF Authentifizierungsdaten von der HSS durch Senden einer Cx-Multimedia-Ruth-Request MAR mit der IMPI. Dazu wird auf 3GPP TS 29.229 verwiesen.
4. Die HSS antwortet mit einer Multimedia-Ruth-Antwort MAA, welche den ersten Schlüssel DK für das HTTP-Digest.
5. Die S-CSCF generiert den zweiten Schlüssel NK mittels der vorbestimmten Funktion F unter Verwendung von DK und Nonce als Eingangsparameter. Die S-CSCF indiziert der P-CSCF über die I-CSCF mittels einer SIP-401-Unauthorized-Nachricht, dass die HTTP-Digest-Authentifizierung angefragt wurde. Die SIP-401-Unauthorized-Nachricht enthält einen WWW-Authenticate-Header mit der Nonce. Zusätzlich wird der zweite Schlüssel NK zur P-CSCF transportiert, sodass das Schlüssel-Management-Protokoll ausgeführt werden kann.
6. Die P-CSCF kann den zweiten Schlüssel NK speichern und leitet die SIP-401-Unauthorized-Nachricht zu der Teilnehmereinrichtung UE1, allerdings ohne den zweiten Schlüssel NK. Der gespeicherte zweite Schlüssel NK darf nicht durch die P-CSCF verwendet werden, solange der Registrierungs-Prozess nicht erfolgreich beendet ist (ab Schritt 9 gemäß Fig. 5 kann NK verwendet werden).
7. Die Teilnehmereinrichtung UE1 berechnet den Digest-Wert Digest unter Verwendung des gespeicherten ersten Schlüssels DK und der empfangenen Nonce. Die Teilnehmereinrichtung UE1 sendet eine zweite SIP-Register-Anfrage zur P-CSCF, welche einen Authorisierungs-Header beinhaltet, der die IMPI und den kalkulierten Digest-Wert Digest aufweist.
8. Die P-CSCF leitet die empfangene Nachricht über die I-CSCF an die S-CSCF weiter.
9. Nachdem die S-CSCF diese Nachricht empfangen hat, berechnet sie erneut den Digest-Wert Digest unter Verwendung des gespeicherten Schlüssels DK, den sie vorher von der HSS empfangen hat, als Digest-Schlüssel und der Nonce. Die S-CSCF vergleicht den berechneten Digest-Wert Digest mit dem von der Teilnehmereinrichtung UE1 empfangenen Digest-Wert Digest. Falls beide übereinstimmen, ist die Registrierung durch Senden einer SIP-200-OK-Nachricht an die Teilnehmereinrichtung UE1 erfolgreich beendet. Wenn die 200-OK-Nachricht die P-CSCF passiert, kann die P-CSCF ebenfalls eine erfolgreiche Komplettierung des Registrierungsprozesses annehmen und kann von da ab den zweiten Schlüssel NK, den sie in Schritt 6 gespeichert hat, verwenden.
10. Falls beispielsweise die Teilnehmereinrichtung UE1 eine verschlüsselte Sitzung haben möchte, kann sie einen verschlüsselten Hauptschlüssel enc(MK) in der SIP-Invite-Nachricht (siehe Nachricht 10 gemäß Fig. 5) an die P-CSCF übertragen. Die Verschlüsselung des Hauptschlüssels MK in den verschlüsselten Hauptschlüssel enc(MK) wird mittels des zweiten symmetrischen Schlüssels NK durchgeführt. Nachdem der zweite Schlüssel NK der P-CSCF bekannt ist, kann diese den empfangenen, verschlüsselten Hauptschlüssel enc(MK) entschlüsseln.
11. Die Initiierung der Sitzung wird durch Senden der zweiten SIP-OK-Nachricht zurück zur Teilnehmereinrichtung UE1 bestätigt.

[0074] Ab Schritt 10 in Fig. 5 ist eine Initiierung der Sitzung durch die Teilnehmereinrichtung UE1 durchgeführt. Alternativ kann die Initiierung der Sitzung auch durch die Provider-Einrichtung PE1, dabei insbesondere durch die P-CSCF erfolgen.

[0075] Fig. 6 zeigt ein schematisches Ablaufdiagramm des erfindungsgemäßen Verfahrens für Beispiel 1 mit Alternative 2. Das vierte Ausführungsbeispiel gemäß Fig. 6 unterscheidet sich von dem dritten Ausführungsbeispiel gemäß Fig. 5 in Schritt 4. Schritt 4 in Fig. 6 ist dahingehend unterschiedlich zu Schritt 4 in Fig. 5, dass die HSS gemäß Fig. 6 nur den zweiten Schlüssel NK und nicht direkt den ersten Schlüssel DK versendet. Zusätzlich wird noch der erwartete Digest-Wert Digest zur S-CSCF gesendet.

[0076] Obwohl die vorliegende Erfindung vorstehend anhand der bevorzugten Ausführungsbeispiele beschrieben wurde, ist sie darauf nicht beschränkt, sondern auf vielfältige Art und Weise modifizierbar. Beispielsweise ist es denkbar, den Schlüssel NK erst in der 200 OK Nachricht von der S-CSCF zur P-CSCF zu senden. Des Weiteren ist es denkbar, die Erfindung auf eine Nicht-IMS-Architektur anzuwenden. In einer solchen Nicht-IMS-Architektur kann der SIP-Proxy direkt mit dem ersten symmetrischen Schlüssel DK ausgestattet werden, sodass ein Empfangen des ersten Schlüssels DK von einer Datenbank oder ein Transfer des zweiten Schlüssels NK

von S-CSCF/HSS zur P-CSCF nicht notwendig wird.

Patentansprüche

1. Verfahren zum Bereitstellen eines symmetrischen Schlüssels (NK) zum Sichern eines Schlüssel-Management-Protokolls, mittels welchem kryptographisches Material für ein Protokoll zum verschlüsselten Übertragen von Mediendaten (MD) zwischen einer Teilnehmereinrichtung (UE1) und einer Provider-Einrichtung (PE1) generiert wird, mit den Schritten:
(a) Bereitstellen eines ersten symmetrischen Schlüssels (DK) der Teilnehmereinrichtung (UE1) und der Provider-Einrichtung (PE1), welcher in einem auf symmetrischen Schlüsseln basierenden Sicherungsmechanismus eines Netzprotokolls einer Kontrollschicht zum Aufbau einer Kommunikationssitzung zwischen der Teilnehmereinrichtung (UE1) und der Provider-Einrichtung (PE1) eingesetzt wird;
(b) Bereitstellen eines ersten zeitveränderlichen Parameters (Nonce) durch die Provider-Einrichtung (PE1);
(c) Übertragen des bereitgestellten ersten zeitveränderlichen Parameters (Nonce) von der Provider-Einrichtung (PE1) an die Teilnehmereinrichtung (UE1);
(d) Berechnen eines zweiten symmetrischen Schlüssels (NK) für das Sichern des Schlüssel-Management-Protokolls mittels einer vorbestimmten Funktion (F) in Abhängigkeit zumindest des bereitgestellten ersten symmetrischen Schlüssels (DK) und des bereitgestellten ersten zeitveränderlichen Parameters (Nonce) durch die Provider-Einrichtung (PE1); und
(e) Berechnen des zweiten symmetrischen Schlüssels (NK) mittels der vorbestimmten Funktion (F) in Abhängigkeit zumindest des bereitgestellten ersten symmetrischen Schlüssels (DK) und des übertragenen ersten zeitveränderlichen Parameters (Nonce) durch die Teilnehmereinrichtung (UE1).

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass das Protokoll zum verschlüsselten Übertragen der Mediendaten (MD) als Secure-Real-Time-Transport-Protocol (SRTP) und/oder
das Schlüssel-Management-Protokoll als Multimedia-Internet-Keying (MIKEY) und/oder
der Sicherungsmechanismus als Authentifizierungs- und/oder Integritätsprotokoll, insbesondere als HTTP-Digest-Protokoll, und/oder
das Netzprotokoll zum Aufbau der Kommunikationsverbindung als Session-Initiation-Protocol (SIP) ausgebildet sind/ist und/oder
das kryptographische Material einen Hauptschüssel zur Ableitung von Sitzungsschlüsseln und kryptographischen Kontext aufweist.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass das Schlüssel-Management-Protokoll in der Kontrollschicht und/oder in einer Medienschicht eingesetzt wird.

4. Verfahren nach Anspruch 1 oder einem der Ansprüche 2 oder 3,
dadurch gekennzeichnet,
dass das Verfahren weiter folgende Schritte aufweist:
– Generieren eines zweiten zeitveränderlichen Parameters (CNonce) durch die Teilnehmereinrichtung (UE1);
– Übertragen des generierten zweiten zeitveränderlichen Parameters (CNonce) von der Teilnehmereinrichtung (UE1) an die Provider-Einrichtung (PE1)
– Berechnen des zweiten symmetrischen Schlüssels (NK) in Abhängigkeit des bereitgestellten ersten symmetrischen Schlüssels (DK), des bereitgestellten ersten zeitveränderlichen Parameters (Nonce) und des von der Teilnehmereinrichtung (UE1) übertragenen, zweiten zeitveränderlichen Parameters (CNonce) durch die Provider-Einrichtung (PE1); und
– Berechnen des zweiten symmetrischen Schlüssels (NK) in Abhängigkeit des bereitgestellten ersten symmetrischen Schlüssels (DK), des von der Provider-Einrichtung (PE1) übertragenen ersten zeitveränderlichen Parameters (Nonce) und des generierten, zweiten zeitveränderlichen Parameters (CNonce) durch die Teilnehmereinrichtung (UE1).

5. Verfahren nach Anspruch 1 oder einem der Ansprüche 2–4, dadurch gekennzeichnet, dass ein dritter zeitveränderlicher Parameter (Nonce-Count) jeweils durch die Teilnehmereinrichtung (UE1) und die Provider-Einrichtung (PE1) von dem ersten zeitveränderlichen Parameter (Nonce) abgeleitet wird, in dessen Abhängigkeit der zweite symmetrische Schlüssel (NK) jeweils durch die Teilnehmereinrichtung (UE1) und die Provider-Einrichtung (PE1) berechnet wird.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass der erste zeitveränderliche Parameter (Nonce) als eine Number-Used-Once (Nonce) und/oder der zweite zeitveränderliche Parameter als eine Client-Defined-Nonce (CNonce) und/oder der dritte zeitveränderliche Parameter als ein Nonce-Count des HTTP-Digest-Protokolls ausgebildet sind/ist.

7. Verfahren nach einem der Ansprüche 4–6, dadurch gekennzeichnet, dass die vorbestimmte Funktion (F) in eine erste Teil-Funktion (F1) und in eine zweite Teil-Funktion (F2) teilbar ist, wobei die erste Teil-Funktion (F1) zumindest den ersten symmetrischen Schlüssel (DK) und den ersten zeitveränderlichen Parameter (Nonce) als Eingangsparameter hat und die zweite Teil-Funktion (F2) zumindest ein Ergebnis der ersten Teil-Funktion (F1(DK, Nonce)) und den zweiten zeitveränderlichen Parameter (CNonce) als Eingangsparameter hat.

8. Verfahren nach Anspruch 1 oder einem der

Ansprüche 2–7, dadurch gekennzeichnet, dass die Teilnehmereinrichtung (UE1) und die Provider-Einrichtung (PE1) zumindest teilweise ein IP-Multimedia-Subsystem (IMS) ausbilden.

9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet,
dass die Provider-Einrichtung (PE1) des IP-Multimedia-Subsystems (IMS) aufweist:
– eine Proxy-Funktionalitätseinheit (P-CSCF), welche mit der Teilnehmereinrichtung (UE1) gekoppelt ist,
und/oder
– eine Interrogations-Funktionalitätseinheit (I-CSCF), welche mit der Proxy-Funktionalitätseinheit (P-CSCF) gekoppelt ist,
und/oder
– eine Server-Funktionalitätseinheit (S-CSCF), welche mit der Interrogations-Funktionalitätseinheit (I-CSCF) gekoppelt ist
und/oder
– eine Home-Subscriber-Server-Einheit (HSS), welche mit der Server-Funktionalitätseinheit (S-CSCF) gekoppelt ist und zumindest den ersten symmetrischen Schlüssel (DK) speichert.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass das HTTP-Digest-Protokoll zwischen der Teilnehmereinrichtung (UE1) und der Server-Funktionalitätseinheit (S-CSCF) ausgeführt wird.

11. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass das HTTP-Digest-Protokoll zwischen der Teilnehmereinrichtung (UE1) und der Home-Subscriber-Server-Einheit (HSS) ausgeführt wird.

12. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die erste Teil-Funktion (F1) von der Server-Funktionalitätseinheit (S-CSCF) ausgeführt wird, das Ergebnis der ersten Teil-Funktion (F1(DK, Nonce)) von der Server-Funktionalitätseinheit (S-CSCF) an die Proxy-Funktionalitätseinheit (P-CSCF) übertragen wird, der zweite zeitveränderliche Parameter (CNonce) von der Proxy-Funktionalitätseinheit (P-CSCF) empfangen wird und die zweite Teil-Funktion (F2) von der Proxy-Funktionalitätseinheit (P-CSCF) ausgeführt wird.

13. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass die erste Teil-Funktion (F1) von der Home-Subscriber-Server-Einheit (HSS) ausgeführt wird, das Ergebnis (F1(DK, Nonce)) der ersten Teil-Funktion (F1) von der Home-Subscriber-Server-Einheit (HSS) an die Proxy-Funktionalitätseinheit (P-CSCF) übertragen wird, der zweite zeitveränderliche Parameter (CNonce) von der Proxy-Funktionalitätseinheit (P-CSCF) empfangen wird und die zweite Teil-Funktion (F2) von der Proxy-Funktionalitätseinheit (P-CSCF) ausgeführt wird.

14. Verfahren nach Anspruch 1 oder einem der Ansprüche 2 bis 13, dadurch gekennzeichnet, dass die Teilnehmereinrichtung (UE1) eine SIP-basierte Subskription mit der Provider-Einrichtung (PE1) hat.

15. Verfahren zum Verschlüsseln von Mediendaten (MD) zwischen einer Teilnehmereinrichtung (UE1) und einer Provider-Einrichtung (PE1) mit den Schritten:
– Bereitstellen eines symmetrischen Schlüssels (NK) jeweils zur Teilnehmereinrichtung (UE1) und der Provider-Einrichtung (PE1) mittels des Verfahrens nach Anspruch 1 oder einem oder mehreren der Ansprüche 2 bis 14;
– Verschlüsseln der Mediendaten (MD) in Abhängigkeit des bereitgestellten symmetrischen Schlüssels (NK) durch die Teilnehmereinrichtung (UE1) oder Provider-Einrichtung (PE1);
– Senden der verschlüsselten Mediendaten (MD);
– Empfangen der verschlüsselten Mediendaten durch die Provider-Einrichtung (PE1) oder Teilnehmereinrichtung (UE1); und
– Entschlüsseln der empfangenen Mediendaten (MD) mittels des bereitgestellten symmetrischen Schlüssels (MK) durch die Provider-Einrichtung (PE1) oder durch die Teilnehmereinrichtung (UE1).

Es folgen 5 Blatt Zeichnungen

Anhängende Zeichnungen

FIG 1

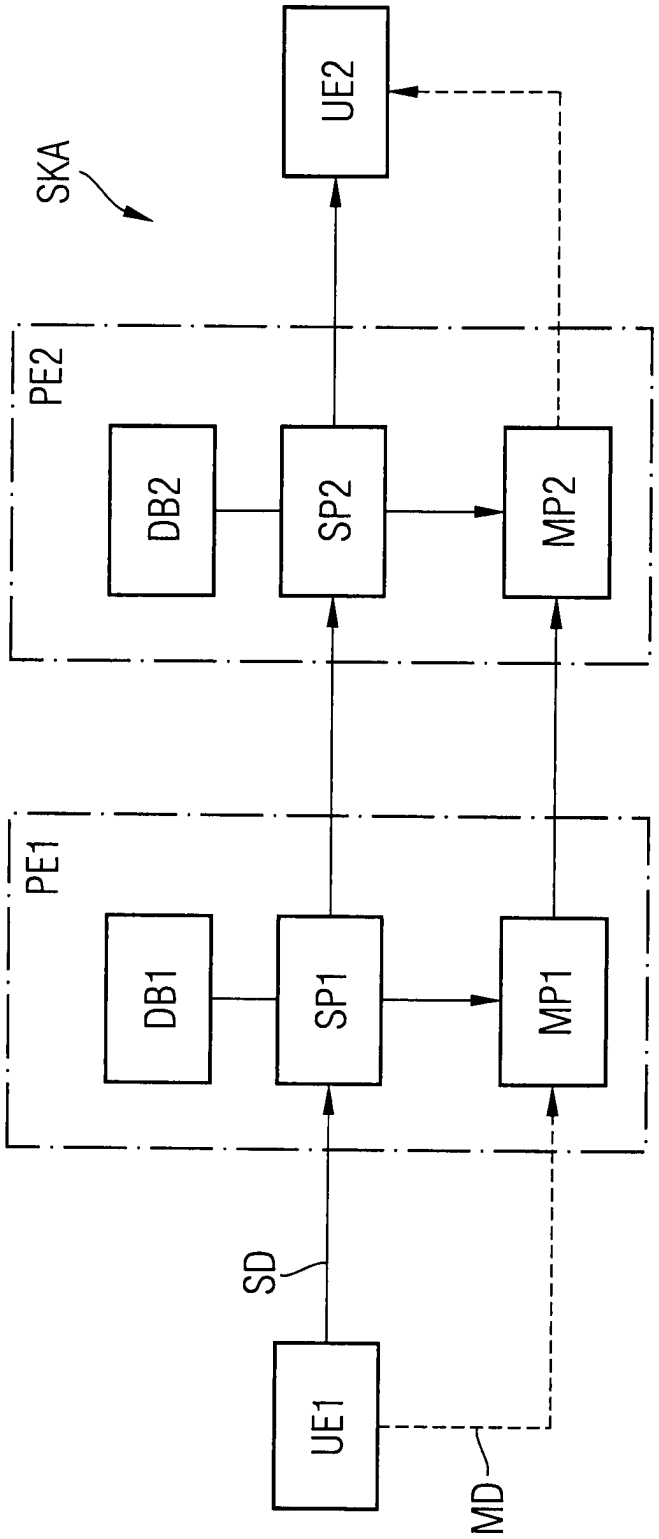


FIG 2

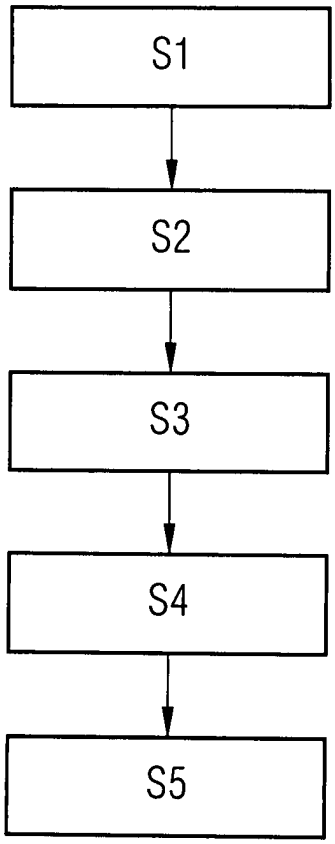


FIG 3

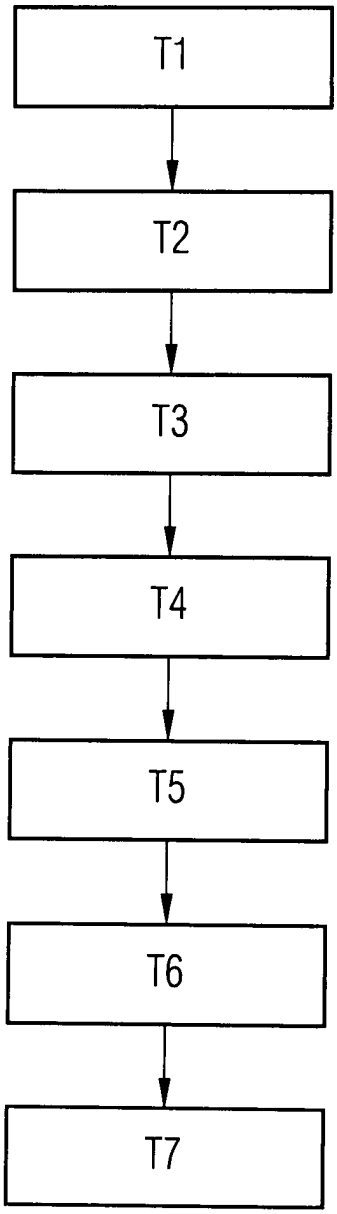
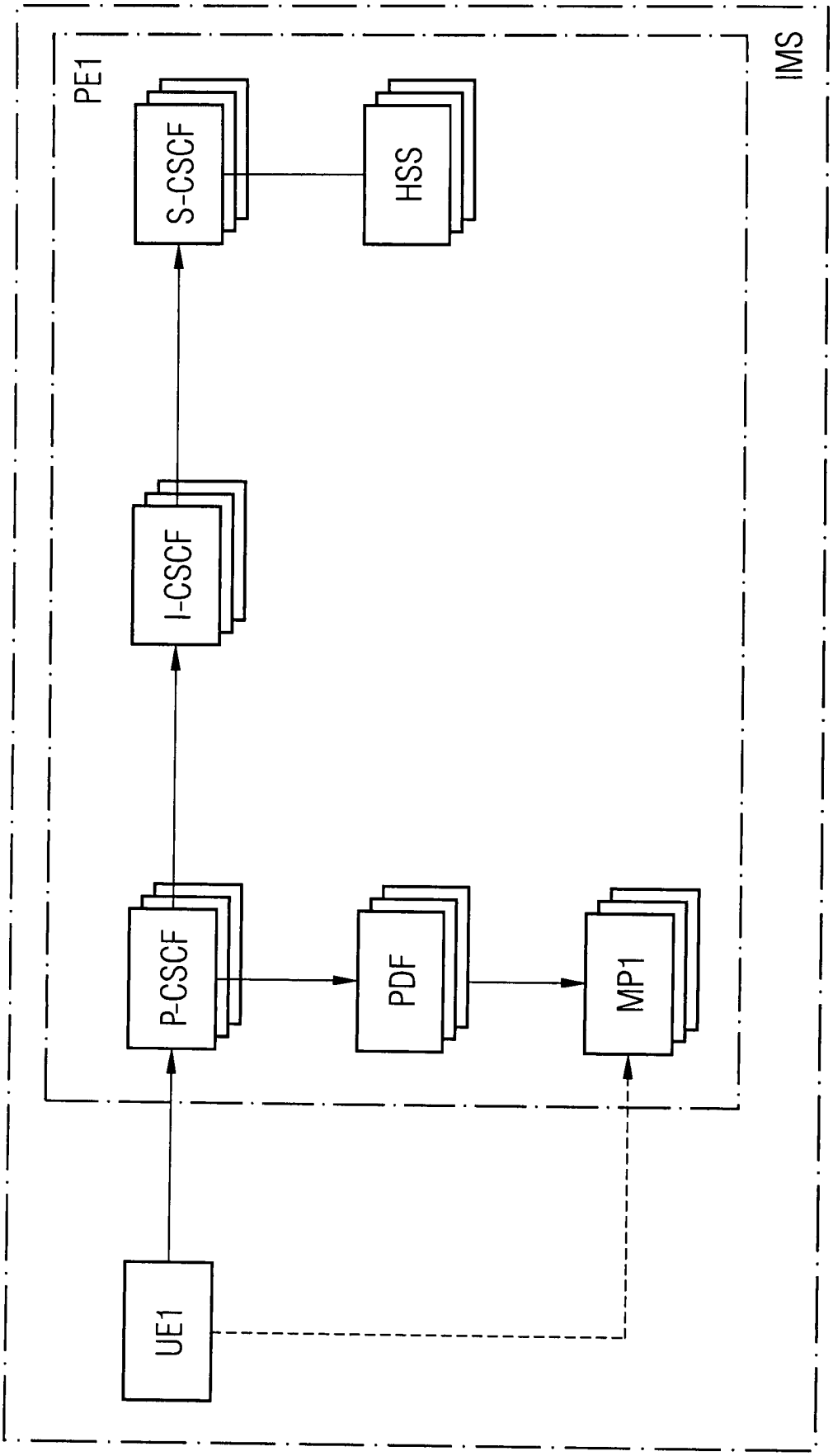


FIG 4



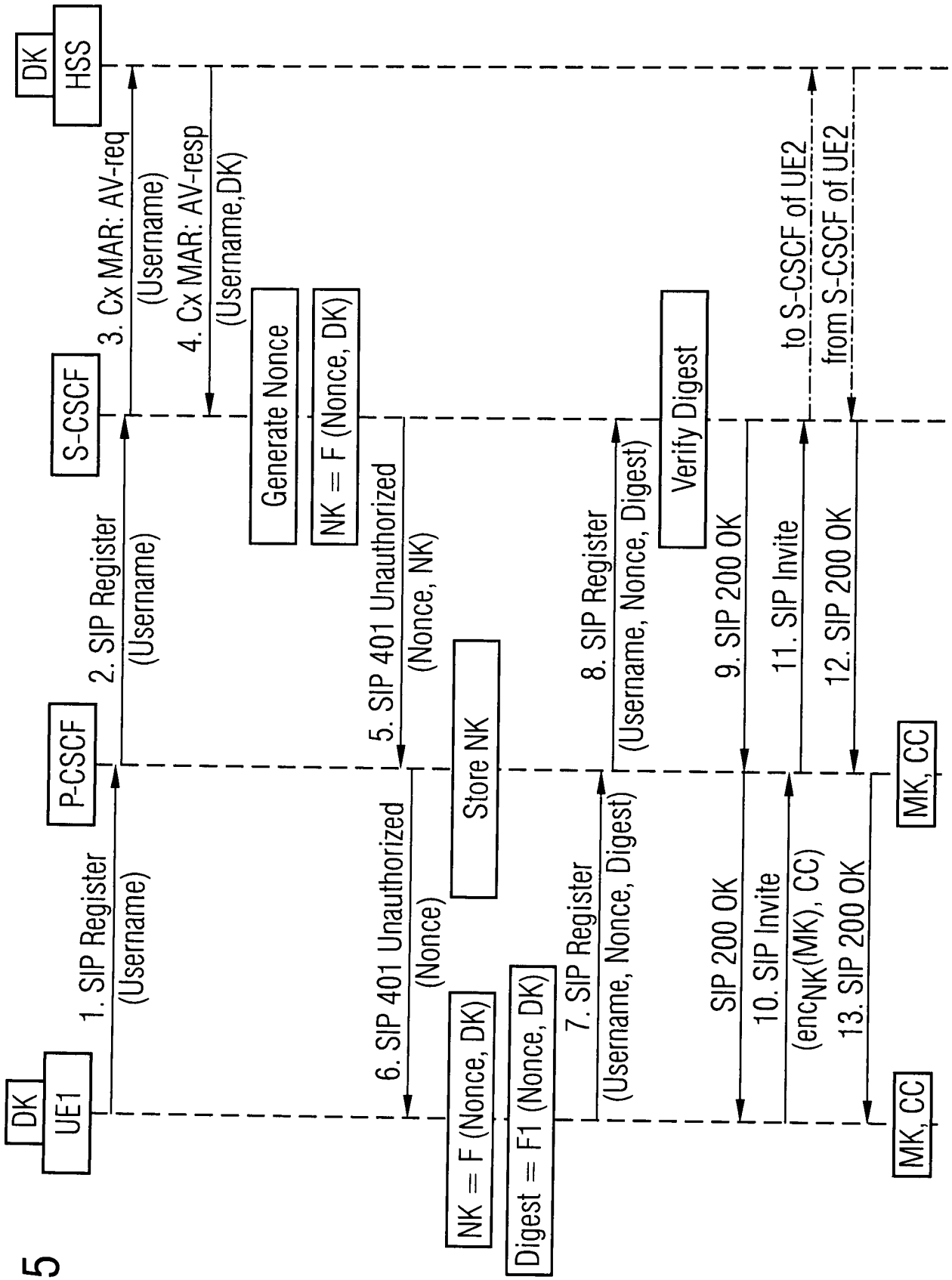

DK
HSS
S-CSCF
P-CSCF
DK
UE1
1. SIP Register
(Username)
2. SIP Register
(Username)
3. Cx MAR: AV-req
(Username)
4. Cx MAR: AV-resp
(Username,DK)
Generate Nonce
NK = F (Nonce, DK)
5. SIP 401 Unauthorized
(Nonce, NK)
Store NK
6. SIP 401 Unauthorized
(Nonce)
NK = F (Nonce, DK)
Digest = F1 (Nonce, DK)
7. SIP Register
(Username, Nonce, Digest)
8. SIP Register
(Username, Nonce, Digest)
Verify Digest
9. SIP 200 OK
SIP 200 OK
10. SIP Invite
(encNK(MK), CC)
11. SIP Invite
to S-CSCF of UE2
12. SIP 200 OK
from S-CSCF of UE2
13. SIP 200 OK
MK, CC
MK, CC

FIG 5

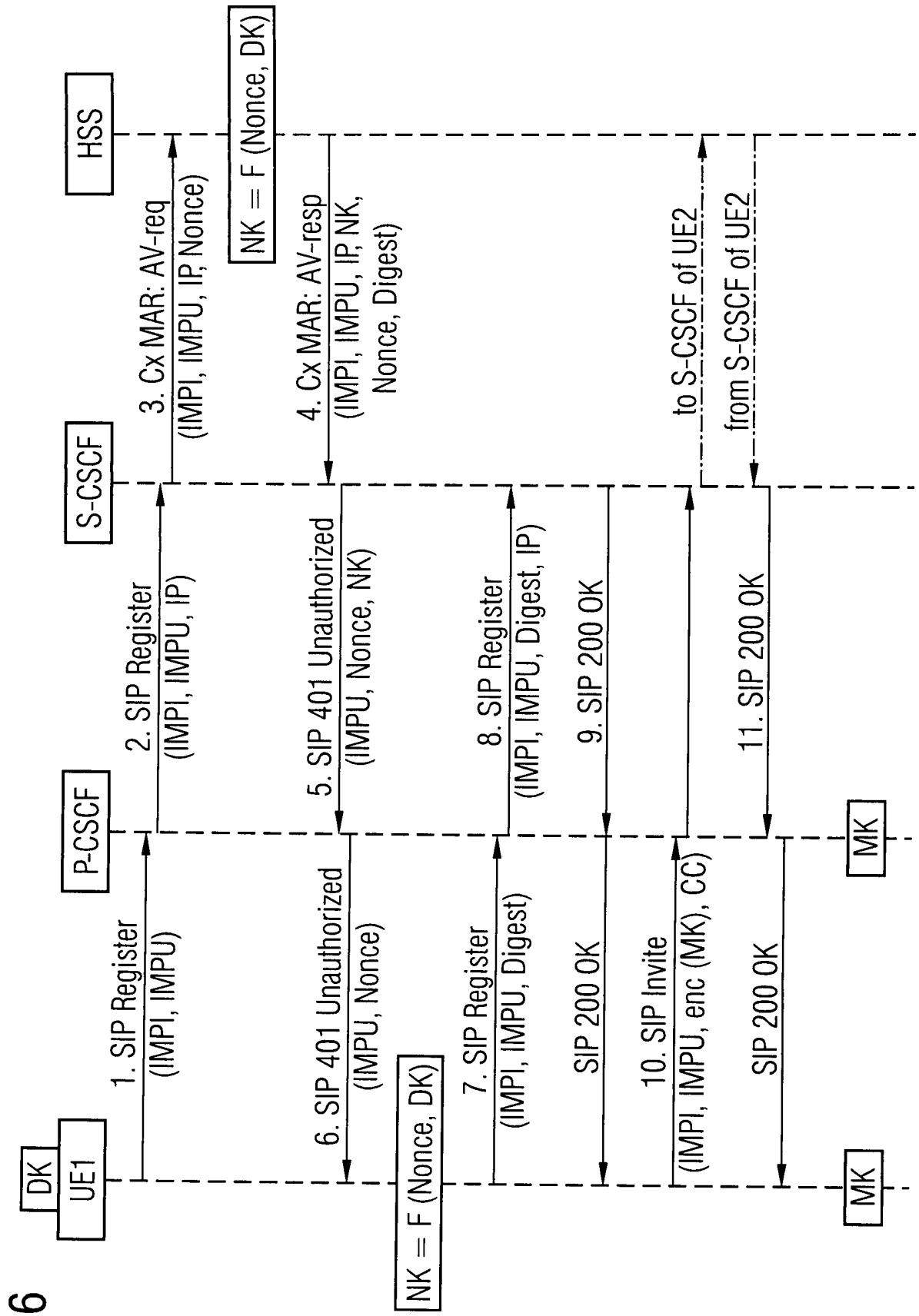

DK
UE1
P-CSCF
S-CSCF
HSS
1. SIP Register
(IMPI, IMPU)
2. SIP Register
(IMPI, IMPU, IP)
3. Cx MAR: AV-req
(IMPI, IMPU, IP, Nonce)
NK = F (Nonce, DK)
4. Cx MAR: AV-resp
(IMPI, IMPU, IP, NK,
Nonce, Digest)
5. SIP 401 Unauthorized
(IMPU, Nonce, NK)
6. SIP 401 Unauthorized
(IMPU, Nonce)
NK = F (Nonce, DK)
7. SIP Register
(IMPI, IMPU, Digest)
8. SIP Register
(IMPI, IMPU, Digest, IP)
SIP 200 OK
9. SIP 200 OK
10. SIP Invite
(IMPI, IMPU, enc (MK), CC)
to S-CSCF of UE2
from S-CSCF of UE2
SIP 200 OK
11. SIP 200 OK
MK
MK

FIG 6