(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2006 025 369 A1** 2007.06.06

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2006 025 369.8**
(22) Anmeldetag: **31.05.2006**
(43) Offenlegungstag: **06.06.2007**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)
H04L 29/06 (2006.01)
H04L 12/56 (2006.01)

(66) Innere Priorität:
10 2005 057 714.8 02.12.2005

(71) Anmelder:
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., 80686 München, DE

(72) Erfinder:
Schmidt, Andreas, Dr., 65929 Frankfurt, DE; Kuntze, Nicolai, 64293 Darmstadt, DE; Hett, Christian, Dipl.-Inform., 61194 Niddatal, DE

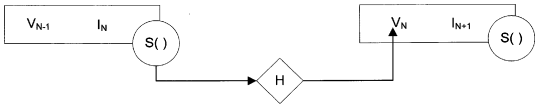
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
US2005/02 65 349 A1
BAUGHER,M., et.al.: RFC 3711, The Secure Real-time Transport Protocol SRTP. März 2004, S.1-56;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gemäß § 44 PatG ist gestellt.

(54) Bezeichnung: **Verfahren und Vorrichtung zur Sicherung der Integrität und/oder Nichtabstreitbarkeit von paketbasierter, zeitkritischer Kommunkation**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren und eine technische Vorrichtung zur Sicherung einer zeitkritischen, ein-, zwei- oder mehrseitigen und zumindest während eines Teilabschnitts der Übertragungsstrecke digitalen, paketbasierten Kommunikation, z.B. Voice over IP, Videokonferenz oder textbasierte Chats, zwischen mind. zwei Personen und/oder Maschinen, dadurch gekennzeichnet, dass die Integrität und/oder Nichtabstreitbarkeit für die Inhalte und/oder den Zeitpunkt und/oder den Ort und/oder die Identität der Gesprächspartner der Kommunikation durch eine während bestimmter Teile oder der gesamten Dauer der Kommunikation paketbasierten Anwendung digitaler technischer Sicherungsmethoden, wie beispielsweise digitale Signierung oder Authentisierung, gewährleistet wird.



Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf die Sicherung einer zeitkritischen, ein-, zwei- oder mehrseitigen und zumindest während eines Teilabschnitts der Übertragungsstrecke digitalen, paketbasierten Kommunikation zwischen mind. zwei Personen und/oder Maschinen.

[0002] Das neueste Beispiel für die immer weiter voranschreitende Konvergenz der Informationstechnologie ist das Transportieren von Sprache über das Internet-Protokoll (Voice over IP, VoIP). Analysten erwarten eine jährliche Wachstumsrate von 20% bis 45% pro Jahr. Der Anteil der (im vereinigten Königreich) über VoIP geführten geschäftlichen Telefonate werde in wenigen Jahren auf über 50% wachsen. Der Erfolg von VoIP wird nicht nur auf Kabelnetze beschränkt bleiben, sondern konvergente Übertragung von Sprache und Daten wird auch die nächste Generation der Mobilfunknetze beeinflussen. Diese neue Technologie bringt allerdings einige Sicherheitsbelange mit sich: Um einen traditionellen leitungsvermittelten digitalen oder analogen Anruf abzuhören oder zu verfälschen, muss ein Angreifer physikalischen Zugriff auf das Transportmedium erlangen. Digitale Netzwerke sind im Allgemeinen wegen ihrer Offenheit und Möglichkeiten zu unbemerkter Manipulation weniger widerstandsfähig gegen solche Angriffe. Dies trifft bereits auf ISDN zu und in einem wesentlich größeren Umfang auf digitale, paketbasierte Netzwerke, zum Beispiel auf IP-Netzwerke. Anstrengungen, den VoIP-Produkten Sicherheits-Funktionen hinzuzufügen sind derzeit ungenügend, auch wenn Vorschläge für den Schutz der Privatsphäre existieren. Aus dem Stand der Technik sind Protokolle wie SRTP (Secure Real Time Transport Protocol) bekannt, die Ende-zu-Ende Abhörsicherheit für Telefonate bieten können und sie von der Sicherheit des Transportmediums und des Kommunikationsanbieters unabhängig zu machen. Diese Protokolle sichern allerdings nur die Abhörsicherheit, gewährleisten aber nicht die Nichtabstreitbarkeit der Kommunikation, insbesondere deren Inhalt, Kommunikationsteilnehmer, Datum und Uhrzeit. Diese Erfindung befasst sich weniger mit Sicherheitsverfahren zum Schutz gegen das Abhören von Kommunikation, sondern mit dem Schutz gegen Verfälschungen der Kommunikationsinhalte. Dies ist zum Beispiel im Bereich von Telefonbanking ein wichtiger Aspekt. Hierbei werden Anweisungen, z.B. Überweisungen, des Bankkunden per Telefon an die Bank gegeben. Eine weitere Anwendung ist die Vertragsverhandlung über Telefon oder Videokonferenz. Wünschenswert wäre die Möglichkeit einer Sicherheitstechnik, die die Integrität und/oder die Nichtabstreitbarkeit der Kommunikation sichert entsprechend eines mündlichen Vertrages mit Zeugen. Eine entsprechende Technik ist bisher nicht bekannt.

[0003] Wird das Gespräch über VoIP geführt so wäre es relativ einfach möglich, während des Gesprächs ohne Wissen der Kommunikationspartner das Gespräch zu verfälschen.

[0004] Auf der anderen Seite bieten Sprach-Unterhaltungen inhärente Beweiskraft durch die Möglichkeit der forensischen Bewertung und Untersuchung der enthaltenen biometrischen Daten, z.B. als unabhängige Art der Sprecher-Authentifikation. Die Möglichkeiten für letzteres sind weit fortgeschritten, wodurch aufgezeichnete analoge Sprachkommunikation eine sehr hohe Beweiskraft erlangt, z.B. vor Gericht.

[0005] Eine Absicherung des Inhaltes von VoIP-Gesprächen über beispielsweise kryptographische Verfahren ist wünschenswert und würde einen deutlichen Vorsprung gegenüber bisherigen Systemen wie ISDN darstellen. Hierdurch kann eine Sicherheit der Verbindung (in Verbindung mit Vertraulichkeit schützenden Protokollen) erreicht werden, die unabhängig ist von der Dienstleistung die der Netzbetreiber zur Verfügung stellt. Dies kann besonders in mobilen Netzwerken von Bedeutung sein.

[0006] Daher wird in der hier vorgestellten Methode die Kommunikation zwischen Parteien auf einer Transaktionsebene betrachtet, für die eine Nichtabstreitbarkeit erreicht wird. Diese Nichtabstreitbarkeit ist eng mit dem Sicherheitsziel der Integrität verbunden. Es muss sichergestellt werden, dass eine Kommunikation nicht verändert wurde weder zu irgendeinem Zeitpunkt während der Übermittlung noch danach. Diese Eigenschaft muss sich auch auf die Zusatzdaten der Kommunikation beziehen, die während der Kommunikation erzeugt oder verwendet werden.

[0007] Der Anwendungsbereich der vorliegenden Erfindung geht in voller Allgemeinheit über den primären Anwendungsbereich paketbasierte, digitale Sprachkommunikation, für die VoIP das bekannteste Beispiel ist, hinaus. Denn wesentlich für die Anwendbarkeit der erfundenen Methoden ist nicht die Art der in der Kommunikation verwendeten Mediendaten, sondern dass es sich um eine (ein-, zwei- oder mehrseitige) Kommunikation im Sinne der Kommunikations- und Sprachtheorie zwischen Partnern handelt. Wesentlich ist, dass die Partner einen bestimmten Grad der Nichtabstreitbarkeit für die Inhalte der durchgeführten Kommunikation erreichen möchten. Für die Anwendbarkeit der entworfenen Technik ist die Paketbasierung wesentliche Bedingung. Nicht wesentlich und im Allgemeinen beliebig ist die Art der in der Kommunikation benutzten Medien und ihrer spezifischen Übertragung. Das heißt zum Beispiel, dass der Anwendungsbereich der Erfindung auch Videodaten, Bildtelefonie, textbasierte Chats und so weiter umfassen kann, sowie auch paketbasierte Medien-Kommunikation die in Zukunft erst erfunden

wird. Ein Beispiel für in der Forschung entwickelte, aber noch nicht in voller Breite am Markt angewandte Kommunikation, die in den genannten Anwendungsbereich fällt, ist z.B. das gemeinsame Arbeiten von Personen, auch an mehreren voneinander entfernten Orten, in dreidimensionalen, virtuellen Konstruktionsumgebungen. Weiterhin ist nicht wesentlich, das natürliche Personen die Kommunikation ausführen. Dies ist schon im Falle der digitalen, paketbasierten Sprachkommunikation wichtig, wo der Anwendungsfall sich natürlich und nur als Beispiel auch auf Ticket-Reservierungs- oder Auskunftssysteme erstreckt, bei denen einer der Kommunikationspartner ein Automat ist. Wesentlich ist in Bezug auf die Anwendbarkeit der Methoden nur das Ziel der Kommunikationspartner, Nichtabstreitbarkeit zu erreichen.

[0008] Es sei angemerkt, dass für nicht zeitkritische Datenübertragungen, wie z.B. E-Mail, digitale Sicherungsmethoden, wie die elektronische Signatur oder Verschlüsselungsverfahren, bereits aus dem Stand der Technik bekannt sind. Hierbei spielt aber der Zeitaspekt und die mehrseitige Kommunikation keine Rolle, ganz im Gegensatz zu den hier betrachteten zeitkritischen Echtzeitanwendungen (auch bekannt als realtime applications), die entsprechend andere Anforderungen an die Sicherungsverfahren stellen.

[0009] Die Aufgabe der vorliegenden Erfindung besteht darin, eine Sicherung einer zeitkritischen, ein-, zwei- oder mehrseitigen und zumindest während eines Teilabschnitts der Übertragungsstrecke digitalen, paketbasierten Kommunikation (im Folgenden mit zpdK abgekürzt) zwischen mind. zwei Personen und/oder Maschinen zu realisieren, so dass die Integrität und/oder Nichtabstreitbarkeit für die Inhalte und/oder den Zeitpunkt und/oder den Ort und/oder die Identität der Gesprächspartner der Kommunikation während bestimmter Teile oder der gesamten Dauer der Kommunikation gewährleistet wird.

[0010] Die Aufgabe wird mit dem Verfahren des unabhängigen Anspruchs 1 gelöst. Vorteilhafte Ausgestaltungen der Verfahren sind Gegenstand der Unteransprüche. Der Anspruch 36 gibt eine Vorrichtung zur Durchführung des Verfahrens aus Anspruch 1 an. Eine vorteilhafte Ausführung der Vorrichtung gibt Anspruch 27 an.

[0011] Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, dass sich der Schutz einer zpdK vor Fälschung und Manipulation vom Schutz der Integrität von anderen Daten dadurch unterscheidet, dass der zeitliche Zusammenhang relevant ist. Insbesondere die Reihenfolge und Verluste der Kommunikationspakete müssen korrekt behandelt werden. Außerdem muss jeder Kommunikation ein Erzeugungszeitpunkt zugeordnet werden. Die Erfindung verwendet zwar bekannte digitale Sicherungsverfahren, wie zum Beispiel die digitale Signatur, wendet diese allerdings in bisher nicht bekannter Art und Weise auf zeitkritische Kommunikationen an.

1) Die Sicherung der Integrität einer zpdK ist eine Grundaufgabe, deren Lösung für alle drei folgenden, anwendungsbezogenen Aufgaben eine wesentliche Voraussetzung ist. Die Lösung von 1) basiert auf einem technischen Grundkonzept mit Erfindungscharakter, das für 2)–4) an die jeweiligen Anforderungen angepasst wird. Die technischen Ausführungsbeispiele von 2)–4) beinhalten demgemäß technische Ausführungsbeispiele von 1).

2) Sichere Archivierung einer zpdK. Digitale Daten unterliegen grundsätzlich weitgehenderen Manipulationsmöglichkeiten als analoge, bei denen Manipulationen stets Spuren hinterlassen. Daher ist eine die Integrität auch über lange Zeiträume sichernde Aufbewahrung digitaler Sprachkommunikation eine Grundvoraussetzung für eine spätere Beweisführung damit.

3) Authentifizierung der Sprecher. Eine Sicherung der Authentizität der Kommunikationsteilnehmer kann durch eine anfangs durchgeführte Authentifikation der Geräte von Anrufer und Angerufenen zusammen mit der inhärenten biometrischen Authentizität der Stimme gelöst werden. Auch wenn man es prinzipiell allein auf der Transportebene lösen könnte, ist es von Vorteil, es mit den Methoden aus 1) und 2) zu kombinieren um den Beweis erbringen zu können, dass ein aufgezeichnetes Gespräch durchgängig mit authentifizierten Geräten von den bezeichneten Sprechern geführt wurde.

4) Elektronische Signaturen über zpdK. Aufbauend auf 1)–3) wird es möglich, für Gespräche das Maß an Nicht-Abstreitbarkeit zu erreichen, das elektronische Signaturen für digitale Dokumente ermöglichen, d.h. eine bewusste Absichtserklärung. Dafür müssen die oben genannten Aufgaben durch den Nachweis, dass man ein vertrauenswürdiges Signatur-Token besitzt ergänzt werden um die ausgesprochene Absicht, zu unterschreiben, auszudrücken. Die rechtliche Wirkung von elektronischen Signaturen erhöht sich, wenn vertrauenswürdige Geräte benutzt werden. Es wird ein entsprechendes technisches Ausführungsbeispiel vorgestellt.

[0012] Ein Vorteil der Erfindung ist, dass in ihrer technischen Ausführung die existierende Infrastruktur größtenteils unberührt gelassen werden kann, da das Grundkonzept eine effiziente und nahtlose Integration in z.B. die secure Internet protocol (SIP)- und realtime transport protocol (RTP)-Protokolle erlaubt. Ein weiterer Vorteil der Erfindung liegt in der effizienten Nutzung von Arbeitsspeicher, Bandbreite, Speicherbedarf und Rechenlast, denn eine zusätzliche Datenübertragung ist bei der vorgestellten Lösung nur in sehr geringem Umfang notwendig. Die zusammengenommenen Vorteile der entwickelten

Technik tragen zu einem neuen Paradigma für die Nicht-Abstreitbarkeit von digitalen Daten bei.

[0013] Die Kombination von Integritätsschutz, Sicherheit von aufgezeichneten digitalen Gesprächen, Sicherheit über die Identität der Dialogpartner und letztlich die Absichtsbekundung verkörpert durch Signaturen ermöglicht rechtlich bindende mündliche Verträge zwischen unbekannten Personen. Prinzipiell ist so für mündliche Verträge die Sicherheit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz erreichbar.

1.2 Anforderungen für die Integrität digitaler Sprachkommunikation

[0014] Die zentralen Anforderungen, um Nicht-Abstreitbarkeit bei der zpdK zu erzielen beziehen sich auf Aspekte der Informationssicherheit. Aus dem wohlbekannten Dreiergespann Vertraulichkeit, Integrität und Verfügbarkeit der Grundforderungen an IT-Sicherheit ist Integrität die hier wesentliche. Es muss sichergestellt werden, dass ein Kommunikationsvorgang zu keinem Zeitpunkt verändert wurde, sei es während der Übertragung oder später. Des Weiteren umfasst Integrität auch die Integrität jeglicher relevanter Zusatz-Daten, die während des Anrufs erzeugt oder benutzt werden, insbesondere also den Daten, die die Gesprächspartner authentifizieren.

[0015] Auf Grund der speziellen Eigenschaften der zpdK bieten nur beide bzw. alle Sprachkanäle gemeinsam den nötigen Kontext um den Inhalt der Kommunikation komplett zu verstehen und um die inhärente Sicherheit zu nutzen, die eine verwobene natürlichsprachige Konversation bietet. Um sicherzustellen, dass Teile des Gesprächs weder mit anderen Teilen ausgetauscht, durch Einfügungen ersetzt werden, noch herausgeschnitten werden können, muss eine besondere Eigenschaft sichergestellt werden. Diese Eigenschaft bezeichnen wir im Folgenden mit dem Begriff Kohäsion. Kohäsion bedeutet, dass die zeitliche Abfolge der Kommunikation und ihrer Richtung Daten sind, deren Integrität auf eine Art geschützt werden muss, die Manipulationen praktisch unmöglich macht, also z.B. durch hinlänglich starke kryptografische Methoden. Kohäsion als zeitbezogenen Eigenschaft bringt eine ergänzende Anforderung mit sich, nämlich das gesicherte Zuweisen eines zeitlichen Zusammenhangs zu einer zpdK. Jede zpdK muss zuverlässig einer bestimmten Zeit zugeordnet werden, die so nah wie möglich am Anfang des Gesprächs liegt. (Man beachte, dass bei z.B. elektronischen Signaturen das Zuweisen eines Signierzeitpunktes eine rechtliche Anforderung für qualifizierte Signaturen ist gemäß des Europäischen Signaturgesetztes und entsprechender nationaler Regelungen). Abweichungen der Zeitbasis sollten während der signierten Konversation minimiert werden.

[0016] Schließlich hängt Kohäsion auch mit den qualitativen Aspekten des Kommunikationskanals zusammen. Bei schriftlichen Dokumenten ist es in Analogie so, dass ein Unterzeichnender gut daran tut, keine Dokumente zu unterschreiben, die unlesbar oder mehrdeutig sind. In der digitalen Domäne entspricht dies dem Präsentationsproblem für elektronisch signierte Daten. Analog dazu muss die Qualität des Kanals der zpdK auf einer Ebene gewährleistet werden, dass für beide Gesprächspartner Verständlichkeit sichergestellt ist in dem Zeitraum, während dem das Gespräch abgesichert werden soll, z.B. in dem eine der der Aufgaben 2)–4) durchgeführt werden soll. Dazu muss jede Architektur, die sich mit Sicherheitsaspekten der zpdK beschäftigt insbesondere Paketverluste angemessen betrachten, und zwar in mit der Kohäsions-Anforderung konsistenter Weise.

[0017] Eine triviale Voraussetzung, damit ein Teilnehmer ein Gespräch als Beweisstück verwenden kann, ist, dass sichergestellt wird, dass das Gespräch später zur Verfügung steht. Weitere, eher praktische Anforderungen betreffen die Effizienz des Systemdesigns und der Implementierung. Erstens ist es sowohl vom Standpunkt der Sicherheit als auch der Effizienz sehr wünschenswert, die zpdK so „nah" wie möglich an ihrer Übertragung und konzeptionell nah am tatsächlich Datenstrom, z.B. dem VoIP-Strom, zu sichern. Eine einfache Implementierung sollte die Auswirkungen auf existierende Systeme und Infrastrukturen minimieren, z.B. sollten Anforderungen an die Client-Seite minimiert werden. Um die Nutzung existierender Infrastruktur ohne oder mit nur geringen Änderungen zu ermöglichen ist eine tiefe Integration erforderlich. Eine effiziente Nutzung von Arbeitsspeicher, Bandbreite, Speicherbedarf und Rechenlast können durch grundsätzliche konzeptionelle Designentscheidungen erreicht werden. Des Weiteren ist eine Skalierbarkeit des Konzepts auf eine große Anzahl an gleichzeitigen Anrufen eine Notwendigkeit in real existierenden Geschäftsumgebungen. Dies bedeutet z.B., dass zentralisierte Infrastrukturen wenn möglich vermieden werden sollen.

2 TA 1) Integrität

[0018] In diesem Abschnitt wird die Grundaufgabe gelöst, die Integrität von zpdK zu sichern. Dazu beschreiben wir vier Methoden deren Zusammenwirken das gewünschte leistet.

2.1 Intervallbildung

[0019] Die Sicherung einzelner Pakete der zpdK, z.B. durch kryptografische Methoden, ist generell nicht praktisch, z.B. würde sie bei über RTP transportierten Paketen einen nicht annehmbaren Overhead erzeugen, was zu deutlichen Ressourcenverschwendungen, etwa in Bezug auf die zur Verfügung stehen-

de Bandbreite, führen würde.

[0020] Um dies zu vermeiden, wird eine einstellbare Zahl von aufeinander folgenden Paketen zu einem so genannten Intervall, z.B. einer Sprachdauer von einer Sekunde entsprechend, zusammengefasst. Die Länge eines Intervalls kann sich nach tatsächlicher Paket-Anzahl oder nach einem zeitlichen Intervall der zpdK bemessen. Erstere Möglichkeit bringt in praktischen Ausführungen den Vorteil mit sich, dass z.B. Zwischenspeicher für Pakete und Feldlängen für Zusatzdaten feste Größen pro Intervall haben können.

[0021] Bei zpdK sind übertragene Pakete üblicherweise mit ihrer Kommunikationsrichtung, unter Umständen auch Angabe von Sender und Empfänger, ausgezeichnet. Dies gilt insbesondere für SIP/RTP-basiertes VoIP. Dies muss bei der Bildung von Intervalldaten und ihrer Sicherung berücksichtigt werden. Prinzipiell ist es nicht erheblich, ob ein Intervall nur Pakete umfasst, die zu einer bestimmten Kommunikationsrichtung gehören. In allen Ausführungsbeispielen der technischen Aufgaben, die unten dargestellt werden, beziehen sich Intervalle jeweils auf eine einzige Kommunikationsrichtung. Dies vereinfacht viele Abläufe und erlaubt es zum Beispiel bei zweiseitiger, gesicherter zpdK die Darstellung der Methoden für Sende- und Empfangsrichtung voneinander zu trennen.

[0022] Zur Sicherung der Integrität wird nun auf jedes einzelne Intervall sowie die für die Anwendung relevanten und während des Intervalls angefallenen (Zusatz-) Metadaten, z.B. die Richtung des zpdK-Stroms in einem Gespräch zwischen zwei Teilnehmern – die zusammen die so genannten Intervalldaten bilden – eine geeignete technische Sicherungsmethode angewendet. Die Sicherung macht die Intervalldaten unverwechselbar und unveränderbar in dem Sinne, dass jede Veränderung sofort bemerkt werden kann.

[0023] Die genannte Sicherung kann zum Beispiel in der Anwendung eines Hash-Algorithmus' auf die Intervalldaten bestehen, eines keyed-hash message authentication codes (HMAC), in der Anbringung einer elektronischen Signatur, oder eines Zeitstempels. Solche Sicherungen beruhen im Allgemeinen auf mathematischen Einwegfunktionen und gelten daher als Kollisionssicher, d.h. sie sind ein wirksames Mittel um die Identität oder Verschiedenheit zweier Datensätze nachzuweisen. Sie sichern somit Datenintegrität. Als weitere Methoden zur Sicherung von Daten werden im Folgenden die allgemein bekannten Techniken elektronischer Signaturen, z.B. beruhend auf asymmetrischer Kryptographie, sowie elektronische Zeitstempel vorausgesetzt und wiederholt benutzt.

[0024] Während der Dauer eines Intervalls kann es je nach zu lösender Aufgabe immer noch nötig sein, Sicherungswerte, z.B. Hash-Werte, jedes einzelnen Pakets zu erzeugen. Diese können wiederum als Zusatzdaten in die Intervalldaten eingehen. Die hier vorgestellten Methoden machen es jedoch prinzipiell nicht nötig, dass Sicherungswerte einzelner Pakete übertragen werden. Wichtig ist anzumerken, dass der Begriff der Intervalldaten eine logische Einheit bezeichnet und nicht etwa ein Datenformat. Insbesondere ist nicht ausgesagt, welche Teile der Intervalldaten zwischen Kommunikationspartnern übertragen werden. Entscheidend für letzteres ist, dass ein Empfänger jeweils in die Lage versetzt wird, die Integrität nachzuprüfen.

[0025] Spezielle Intervalle treten am Anfang bzw. Ende der Sicherung einer zpdK auf. Diese Start- bzw. End-Intervalle tragen entsprechende Kennzeichnungen und weitere Daten wie z.B. Startzeitpunkt, Grund des Gesprächsendes (Auflegen, Abbruch durch Fehler, oder ähnliches). Das Start-Intervall kann, muss aber nicht unbedingt Sprachdaten umfassen.

2.2 Verkettung von Intervallen

[0026] Um die Kohäsion der sprachlichen Kommunikation wie gefordert sicherzustellen, reicht die Sicherung der einzelnen Intervalle oft nicht aus. Vielmehr muss verhindert werden, dass Intervalle von einem Angreifer ersetzt oder herausgeschnitten werden.

[0027] Kohäsion im beschriebenen Sinne wird hier erreicht durch eine Verkettung der Intervalle. Dies geschieht im Grundsatz immer dadurch, dass Sicherungsdaten, die ein bestimmtes Intervall N, sichern, also dessen Inhalte unverwechselbar machen, in die Daten des darauf folgenden Intervalls mit aufgenommen werden.

[0028] Die zur Verkettung verwendeten Daten können dieselben sein, die bereits zur Sicherung von Intervall N benutzt wurden, oder auch eigens für den Zweck der Verkettung gebildete. Zum Beispiel kann man den zur Sicherung von Intervall N verwendeten Hash-Wert nehmen und einfach in Intervall N+1 einfügen. Oder man kann, wo dies die Sicherheit erhöht, einen neuen Hash-Wert über N und ggf. Ns elektronische Signatur bilden und in die Intervalldaten des Intervalls N+1 einfügen.

[0029] Die Verkettung ist schematisch in Fig. 1 gezeigt. Zunächst wird eine erste Sicherungsmethode S(), zum Beispiel eine elektronische Signatur, auf die Intervalldaten I_N und den Sicherungswert des vorhergehenden Intervalls V_{N-1} angewendet. Der zur Verkettung des Intervalls N+1 mit Intervall N benutzte Wert V_N wird gebildet durch Anwendung einer geeigneten Funktion, z.B. eines Hash-Algorithmus, auf $S(I_N, V_{N-1})$ oder auf $S(I_N, V_{N-1})$ und die Intervalldaten I_N und/oder V_{N-1}. Das erste Intervall besitzt keinen Vor-

gänger. Es kann dennoch genau so geformt sein wie die folgenden, indem man den Verkettungswert des letzten Intervalls an der entsprechenden Stelle durch eine nur einmal verwendete Zufallszahl (Nonce) ersetzt. Die Verwendung von Noncen gilt als probate Methode zur Erhöhung der Sicherheit. Sie kann hier dazu dienen, die Kette der Intervalle und damit die gesamte zpdK unverwechselbar zu machen.

[0030] Bei späteren Überprüfungen der Sicherungsdaten und Vergleich mit den tatsächlich vorliegenden zpdK-Paketen lässt sich somit der Beweis über die zugesicherte Eigenschaft, z.B. Signatur eines Gesprächspartners, führen. Im konkreten Fall kann dies zum Beispiel durch Vergleich von in den gesicherten Intervallen enthaltenen Hash-Werten mit neu aus den vorliegenden zpdK-Paketen berechneten geschehen.

2.3 Behandlung von Paketverlusten

[0031] In der zpdK ist die Berücksichtigung von Verlusten und anderen Fehlern auf Paketebene, wie z.B. Pakete die nicht in der richtigen Reihenfolge ankommen, essentiell. Hierzu tragen Pakete üblicherweise (z.B. bei RTP) fortlaufende Nummern. Für die Sicherung der Integrität der zpdK ist wesentlich, das Paketverlust vor der Sicherung toleriert werden muss, danach aber nicht mehr auftreten darf und z.B. nachweisbar gemacht wird.

[0032] In Bezug auf die Verkettung von Intervallen, die jeweils mehrere Pakete enthalten, werden im Folgenden vier grundlegende Möglichkeiten dargestellt, um Paketverlust abzufangen. Bei der Beschreibung dieser Möglichkeiten werden öfters Hash-Werte als Beispiele einer Methode zur Sicherung von Datenintegrität verwendet.

[0033] Die grundsätzliche, erfindungsgemäße Methode zur Behandlung von Paketverlusten ist stets gleich. Es wird von einem Empfänger von zpdK eine Meldung über die tatsächlich empfangenen Pakete erzeugt und an den oder die Sender, oder eine je nach zu lösender Aufgabe zu bestimmenden ausgezeichneten Empfänger gesandt. Diese Meldung kann unter Umständen ebenfalls, z.B. mittels kryptographischer Methoden, abgesichert sein. Die Meldung kann zudem zusätzliche Daten enthalten, die zum Beispiel die Unverfälschtheit der beim Empfänger angekommenen zpdK-Pakete nachprüfbar machen. Die vier grundlegenden Möglichkeiten zur Rückmeldung folgen im Einzelnen.

1. Ein zpdK-Sender bildet für alle von ihm ausgehenden Pakete eines Intervalls Sicherungsmerkmale, z.B. Hash-Werte. Die Sicherungsmethode zur Sicherung eines Intervalls wird dann auf alle Paketsicherungswerte und gegebenenfalls auf weitere Metadaten angewendet. Damit ein Empfänger später die Integrität der zpdK verifizieren kann, muss daher die Übertragung der Paketsicherungswerte verlustfrei erfolgen. Insbesondere muss der Empfänger Paketsicherungswerte aufheben, für die ihm keine Paketdaten vorliegen.
2. Der zpdK-Sender erfährt über einen eigenen Kanal, welche Pakete angekommen sind, z.B. deren Paketnummern. Er muss daraufhin nur die Sicherungswerte für diese Pakete bilden und sie übertragen. Dies kann z.B. eingebettet in die Intervalldaten geschehen. Die Sicherungsmethode zur Sicherung der Intervalldaten wird in diesem Fall auf die Paketsicherungswerte der tatsächlich empfangenen Pakete und gegebenenfalls auf weitere Metadaten angewendet.
3. Der zpdK-Sender überträgt im Unterschied zu 2. keine Sicherungswerte über einzelne Pakete. Er erhält aber wie in 2. Rückmeldung über die pro Intervall angekommenen Pakete und bildet Sicherungswerte über diese. Diese Information gehört dann zu den Intervalldaten und wird somit abgesichert. Die Sicherung der Intervalldaten (z.B. der Hash über sie) umfasst somit die Gesprächsdaten aller angekommenen Pakete (und ausschließlich dieser). Die einzelnen Paketsicherungswerte müssen in diesem Fall nicht übertragen werden, da ein Empfänger sie aus den erhaltenen Paketen rekonstruieren kann.
4. Der zpdK-Sender bildet keine Paketsicherungswerte, sondern fügt die digitalen Daten der Pakete, die ihm als Empfangen gemeldet wurden, in der richtigen Reihenfolge hintereinander. Dieser Datenblock wird den Intervalldaten hinzugefügt und abgesichert, muss aber nicht nochmals übertragen werden.

[0034] Der Empfänger muss in den Möglichkeiten 2., 3. und 4., um die Integrität eines Intervalls zu verifizieren, die Sicherungswerte berechnen die ihm fehlen. Dies sind bei 2. und 3. die Sicherungswerte jedes nach seiner eigenen Meldung übertragenen Pakets, bei 4. der Sicherungswert über die Hintereinanderfügung aller dieser Pakete.

[0035] Modifizierbar ist in 2.–4. der Zeitpunkt der Berechnung der Sicherungswerte der einzelnen Pakete auf Seiten des Senders. Sie kann sofort erfolgen und das einzelne Paket gelöscht werden, oder erst nach Meldung über den Empfang des Pakets. Hierdurch ist z.B. eine Anpassung an vorhandene Ressourcen möglich.

[0036] In den technischen Ausführungsvarianten der Aufgaben 2)–4) wird hier Möglichkeit 2. mit Übertragung der Paket-Hashes bevorzugt. Dies erweist sich als Effizient auf Seiten des Senders, insbesondere in Bezug auf Speicherplatz.

[0037] Andererseits ermöglicht diese Option eine erweiterte forensische Analyse, da beispielsweise bei Verlorengehen eines Pakets, z.B. in einem Archiv

noch dessen Hash als redundante und über die Sicherung der Intervalldaten abgesicherte Information verfügbar ist.

2.4 Sicherheits-Überprüfungen und Politiken

[0038] Protokolle zur Übertragung von Multimediadaten wie RTP bieten einige Ansatzpunkte für Sicherheitsüberprüfungen und -maßnahmen. Diese sind auch im Zusammenspiel mit der vorgestellten Sicherung der zpdK Integrität sinnvoll. Beispielsweise erlaubt SIP/RTP den Einsatz eines Wiedereinspielungsfensters (replay window), welches das Einfügen eines zweiten Datenstromes verhindert. Sequenznummern einzelner Pakete können geprüft werden um die Verlustquote zu überprüfen. Die in den RTP-Paketen enthaltenen Zeitangaben können gegen eine Systemzeit auf Diskrepanzen geprüft werden.

[0039] Darüber hinaus werden nun einige Sicherheitsmassnahmen vorgestellt, die erst im Kontext des vorgestellten Sicherungsverfahrens möglich und sinnvoll werden.

2.4.1 Kanalqualität

[0040] Eine wesentliche Angriffsmöglichkeit auf nach den oben dargestellten Konzepten gesicherte zpdK ist ein gezieltes Unterdrücken von Paketen, d.h. eine künstliche Reduktion der Kanalqualität. Um solchen Angriffen zu begegnen, wird permanent die Kanalqualität/gemessen (dies ist in 2.–4. in Abschnitt 2.3 implizit durch die Rückmeldung der angekommenen Pakete der Fall). Sinkt die Qualität unter einen vorher zu bestimmenden Grenzwert (Unterlauf), so können verschiedene Maßnahmen ergriffen werden, z.B.

1. Der Unterlauf wird ignoriert.
2. Der Unterlauf wird den Kommunikationspartnern signalisiert, aber das Sicherungsverfahren (Intervallverkettung) wird nichtsdestotrotz fortgesetzt.
3. Die Sicherung wird abgebrochen (dies wird in der Regel den Partnern signalisiert).
4. Die Kommunikation wird zwangsweise beendet.

[0041] Es ist eine wesentliche Eigenschaft des vorgestellten Sicherungsverfahrens, das die Durchsetzung dieser Sicherheitspolitiken überhaupt erst ermöglicht wird. Alle Politiken 1.–4. können in Anwendungsfällen sinnvoll werden. 1. und 2. sind dies aber letztlich nur, weil die Sicherungsmethode eine nachgelagerte Überprüfung der Kanalqualität erlaubt.

2.4.2 Bruch der Verkettung

[0042] Die Verkettung der Intervalle führt zu einer Fragilität der gesicherten zpdK. Fehlt ein Intervall oder ist es nicht mehr zu verifizieren, so schlägt auch die Verifikation aller folgenden Intervalle und damit der gesamten späteren Kommunikation fehl. Ein Angreifer könnte Teile der zpdK später Entfernen, ohne das z.B. eine verlusttolerante Signatur bricht, was somit nicht erkennbar wäre. Dies könnte z.B. zu schädlichen Spekulationen über sprachlich (syntaktisch, grammatikalisch, semantisch) mögliche Vervollständigungen des fehlenden Abschnittes Anlass geben. Der Abbruch der Sicherungskette beugt dem vor, da ein ganzes fehlendes Stück am zpdK-Ende kaum spekulativ rekonstruiert werden wird. Die im letzten Abschnitt gezeigte Möglichkeit, die sichernde Verkettung im Falle eines Unterlaufs der Kanalqualität abzubrechen ist in diesem Sinne eine Sollbruchstelle für das Sicherungsverfahren. In den unten vorgestellten Anwendungs- und Ausführungsbeispielen wird daher die Politik 4. aus Abschnitt 2.4.1 favorisiert, die maximale Sicherheit bietet. Dies ist jedoch je nach Anwendungsfall eine zu treffende Entscheidung – z.B. ist 4. keine gute Politik für eingehende Notrufe.

2.4.3 Zeitliche Festlegung

[0043] Für die zeitliche Festlegung einer gesicherten zpdK können mehrere Methoden kombiniert werden. Zum Beispiel können am Anfang und/oder Ende der Kommunikation, insbesondere bei den Start- und End-Intervallen signierte Zeitstempel hinzugefügt werden. Sie können die jeweiligen Intervalldaten umfassen und mit abgesichert werden oder umgekehrt die Sicherungsdaten umfassen. Zwischen Anfangs- und End-Zeitstempel können die in Paketen enthaltenen zeitlichen Informationen auf Drift überprüft werden.

[0044] Zeitstempel sind eine allgemein bekannte Technologie. Sie beruhen auf elektronischen Signaturen (üblicherweise mittels asymmetrischer Kryptographie) die sich zusätzlich zu den signierten Daten auch über einen Vermerk der Uhrzeit und des Datums erstrecken. Wird der Zeitstempel von einer ausreichend vertrauenswürdigen Instanz, einem so genannten (qualifizierten oder akkreditierten) Zeitstempeldienst angebracht, so gestehen ihm entsprechende Gesetze in Deutschland einen besonderen Beweiswert zu. Bei vorliegen eines qualifizierten Zeitstempels über einen Datensatz geht z.B. ein Richter im Rahmen der Anscheinsbeweisregelung davon aus, dass dieser Datensatz zu dem im Zeitstempel bezeichneten Zeitpunkt bestanden hat.

[0045] Wird ein Zeitstempel an ein digitales Dokument angebracht, das von einem Unterzeichner elektronisch signiert wurde und umfasst der Zeitstempel (d.h. die Zeitstempelsignatur) die ursprüngliche Signatur des Dokuments, so ist damit nachweisbar, dass der Unterzeichner spätestens zum bezeichneten Zeitpunkt das Dokument signiert hat.

3. TA 2) Archivierung

[0046] Telefongespräche zu archivieren wird in Geschäftsumgebungen zur späteren Nachweisführung häufig als Notwendigkeit angesehen und ist zum Beispiel im Telefon-Banking und in Call-Centern üblich (die Einwilligung zur Aufzeichnung ist meist eine Klausel der entsprechenden Nutzungsverträge). Bei zpdK, z.B. VoIP, ist es Stand der Technik die ankommenden und ausgehenden VoIP-Ströme direkt auf Massenspeicher zu spielen, ggf. unter Zuhilfenahme von Verschlüsselung auf der Transportebene, z.B. Secure Sockets Layer(SSL).

[0047] Der Beweiswert solcher digitaler Aufzeichnungen scheint jedoch unter Umständen in Frage zu stehen. Dies ist bedingt durch die spurlose Verfälschbarkeit digitaler Daten, zusammen mit den langen Zeiträumen, über die die Aufzeichnungen in einem Archiv verbleiben. Ein Angreifer hätte ggf. genügend Zeit Teile eines Gesprächs zu „schneiden", umzuordnen, oder sogar synthetische Sprache einzufügen. Dabei könnte er durchaus die entsprechenden Datenpakete, z.B. ihre Sequenznummern, geeignet fälschen, so dass die Veränderung nicht auffallen würde.

[0048] Es ist daher wünschenswert, archivierte zpdK stärker zu sichern. Ein sehr einfacher Ansatz wäre es, Gespräche als ganzes zwischenzuspeichern, in ein Archiv-Format, etwa MP3, zu transformieren und dann kryptografisch (HMACs, Hashes, Signaturen) zu sichern und im Archiv abzulegen. Dies bringt unter Gesichtspunkten der Effizienz und Sicherheit etliche Nachteile mit sich. Zunächst verliert die zpdK bei der Transformation in ein Archiv-Format möglicherweise die enthaltene Kontext-Information z.B. über Kanalrichtung und -qualität (Paketverluste, Jitter), sowie Zeitmarken und Sender- und Empfänger-Addressierung. Die Konversion der Audiodaten führt zudem eine weitere Komponente in das Gesamtsystem ein, die Angriffen unterliegen könnte. Zudem ist das Zwischenspeichern von Gesprächen, die ja eine zunächst unbestimmte Dauer haben, mit hohem, schwer kalkulierbarem Speicheraufwand verbunden. Ein so konstruiertes Archivierungssystem würde auch schlecht auf. eine hohe Anzahl gleichzeitiger Anrufe skalierbar sein – der verfügbare Zwischenspeicher wird hier ggf. zu einer festen oberen Schranke. Außerdem ist der Zwischenspeicher ein Ziel für mögliche Angriffe. Schließlich würde – da ein solches Archivsystem die Signatur und evtl. Zeitstempel ja über das gesamte Dokument bilden muss, was erst nach dem Ende des Gesprächs erfolgen würde – ein gewisser Zeitraum bleiben, den ein Angreifer in jedem Fall nutzen kann, um das Gespräch zu verändern, oder Passagen umzukopieren. Er könnte während des Gesprächs anfängliche Teile bereits manipulieren und trotzdem zu einem plausiblen Zeitpunkt ein Sprach-Dokument plausibler Länge im Archiv ablegen. Diese Probleme werden durch die hier vorgestellte Methode verhindert, da diese Fälschungsmöglichkeit nur für die wesentlich kürzere Intervalllänge besteht, die aber nicht ausreichend ist, um ganze Sätze zu verändern.

[0049] Die hier vorgestellte erfindungsgemäße Methode beruht auf der Sicherung der Integrität von zpdK wie sie in Abschnitt 2 entworfen wurde und unterscheidet sich von dem im letzten Absatz skizzierten, naiven Ansatz stark. Mit dem unten vorgestellten Ansatz wird es möglich, den zpdK-Strom direkt und vollständig unter nachweisbarem Erhalt der Kohäsion zu archivieren.

3.1 Beispielarchitektur und Grundkonzept

[0050] Das Hauptmerkmal in der hier gezeigten technischen Realisierung ist, dass nur minimale technische Anforderungen an die verwendeten Kommunikationsendgeräte gestellt werden. In **Fig. 2** wird eine idealisierte zpdK zwischen zwei Kommunikationspartnern A und B gezeigt. Die Beschränkung auf zwei Partner dient der Übersichtlichkeit und ist keine konzeptionelle Einschränkung. Mit der unten gezeigten Methode können auch z.B. Konferenzen mit mehreren Teilnehmern sicher archiviert werden. An einem bestimmten Punkt der Übertragungsstrecke wird die Komponente VSec eingeführt, welche die Kommunikation mithören kann. Hierbei ist zu beachten, dass alle kommunikationsrelevanten Datenpakte hier durch VSec mithörbar sein müssen. VSec als Hauptkomponente, welche das Sicherheitskonzept implementiert, kann somit beispielsweise auf Seiten der Kommunikationsendgeräte, innerhalb der Kommunikationsvermittlungsgeräte oder an anderen Orten positioniert werden. Die Komponente Arc bezeichnet ein Archiv, an das die durch VSec erzeugten Daten übertragen und persistent gespeichert werden. T1 und T2 bezeichnen zusätzliche Zeitstempeldienste, welche eine höhere Resistenz gegen bestimmte Angriffe bieten.

[0051] Arc ist eine logische Komponente, welche die an ein Archiv zu stellenden Langzeitsicherheitsanforderungen erfüllt. Hier bieten verschiedene, bereits auf dem Markt verfügbare Konzepte Lösungen an, welche eine effiziente, sichere, Langzeitarchivierung ermöglichen. VSec und Arc stellen logische Einheiten innerhalb des Konzeptes dar. Diese können integriert in ein System sein, aber müssen nicht notwendigerweise getrennte Komponenten sein. Es ist auch in bestimmten Szenarien sinnvoll, Arc als eine externe Komponente, die sich unter einer getrennten Kontrolle befindet, zu realisieren. Beispielsweise kann Arc eine externe Dienstleistung einer zweiten Firma sein, welche sich auf Archivierungsaufgaben spezialisiert hat oder unter der Kontrolle einer anderen Abteilung mit anderen Vertrauensannahmen stehen. Die logische Separation einer Komponente, die

Funktionen zur Kontrolle und Durchsetzung von Sicherheitspolitiken vereint ist eine Standardmethode im Design von sicheren Systemen. Eine solche Komponente wird in der Literatur als Referenzmonitor bezeichnet.

[0052] VSec wird sich in einer praktischen Implementierung zumeist unter der Kontrolle einer der Kommunikationspartner befinden. Weder die exakte Position noch die technische Methode des Zugriffs auf die Kommunikation werden hier explizit definiert, da sie ohne Auswirkung auf das hier vorgestellte Konzept ist. Spezifische Möglichkeiten hierzu werden unten im ersten Absatz von Abschnitt 3.2 erläutert. VSec wird dort als so genannter Proxy beschrieben, d.h. ein Knoten in einem Kommunikationsnetz der über die reine Vermittlung und Durchleitung von Kommunikation weitere spezifische Aufgaben erfüllt. Traditionell erfüllen Proxies Aufgaben stellvertretend für Nutzer des Kommunikationsnetzes.

[0053] Die Rolle von VSec innerhalb der Kommunikation kann passiv oder aktiv sein, je nachdem, ob VSec lediglich den Datenstrom zum Zwecke der Archivierung verarbeitet, oder z.B. zusätzlich noch die in Kapitel 2.4 eingeführten sicherheitsrelevanten Politiken auf der zpdK durchsetzt.

[0054] Aufgrund der Forderung einer minimalen Auswirkung auf die Kommunikationsendgeräte muss die Kommunikation zwischen den Kommunikationspartnern nicht von Ende zu Ende digital sein. Insbesondere müssen die Kommunikationsendgeräte nicht notwendigerweise digital, z.B. ISDN oder VoIP, sein. Die Voraussetzung zum Einsatz der vorgestellten Methode wird bereits in vielen bestehenden Netzen erfüllt, da hier die notwendige Digitalisierung und Paketorientierung realisiert wurde. Der Einsatz der Methode ist nicht auf den Einsatz zur Sicherung von Ende-zu-Ende Kommunikation beschränkt. Jede paketbasierte, digitale Kommunikation, wie z.B. (Tele-) Konferenzen oder digitale Radioprogramme, ist durch diese Methode absicherbar.

[0055] Die zpdK zwischen A und B ist bidirektional gerichtet und besteht im Allgemeinen aus zwei Kanälen für die Übertragung von Nutz-(Audio-, Video-) und Meta-Daten. Zu Beginn einer Archivierung, z.B. angestoßen durch SIP-Signalisierung, sammelt VSec initiale Daten welche eine Eindeutige Identifizierung (Unverwechselbarkeit) des aufzuzeichnenden Datenstroms ermöglichen. Daraus bildet VSec gemäß Abschnitt 2.1 ein Start-Intervall, dass auf geeignete Weise gesichert wird, in der Regel mittels eines Geheimnisses das nur VSec bekannt ist, oder das sich VSec und Arc teilen. Gemäß Abschnitten 2.2 und 2.3 wird nun von VSec basierend auf dem Start-Intervall eine gesicherte Intervallkette gebildet. Bei Beendigung oder Abbruch der zpdK (z.B. auch nach der Politik 4. aus Abschnitt 2.4.1) wird ein End-Intervall gebildet. Fehlt dieses End-Intervall, so besteht Grund zu der Annahme, dass die Aufzeichnung auf der Übertragungsstrecke zwischen VSec und Arc oder im Archiv selbst manipuliert wurde. Vorteilhaft ist an den hier vorgestellten Verfahren allerdings auch, dass es im Falle eines Ausfalls bis dahin geleistete Aussagen bereits signiert hat.

[0056] Übernimmt VSec eine aktive Rolle in der Durchsetzung von (Sicherheits-)politiken bezüglich der zpdK, so kann VSec z.B. die in 2.4.1 aufgezeigte Funktion der Überwachung der Kanalqualität übernehmen und entsprechende Maßnahmen bei Unterlauf ergreifen. Intervalllänge und Unterlaufs-Grenzwert sind in diesem Fall wichtige freie Parameter des Konzepts, die an die jeweiligen Gegebenheiten anzupassen sind. Im unten gezeigten Ausführungsbeispiel wird die Intervalllänge dynamisch an die zur Verfügung stehende Rechenleistung angepasst. Zu beachten ist, dass die von VSec beobachtete Kanalqualität nicht unbedingt die bei A und B ankommende sein muss, je nach „Entfernung" zwischen diesen drei Parteien. VSec misst im Allgemeinen nur eine obere Schranke der Kanalqualität. In realen Anwendungen kann sich daher eine direkte, verlustfreie Anbindung an die Kommunikationsschnittstellen eines der Teilnehmer (A oder B, je nachdem wem die Aufzeichnung dient) anbieten.

[0057] In einer bestimmten Hinsicht ist das Archiv-Konzept eine Vereinfachung des Grundkonzepts zur Sicherung der zpdK-Integrität aus Abschnitt 2. Nämlich kann hier eine Behandlung von Paketverlusten durch Signalisierung zwischen Sender und Empfänger wie in Abschnitt 2.3 nicht erfolgen, da die Kommunikationsgeräte von A und B (KA und KB) diesbezüglich passive Geräte sind. Paketverluste können nur wie oben gesagt und in Abschnitt 2.4.1 gezeigt behandelt werden.

3.2 Technisches Ausführungsbeispiel

[0058] Die in dem folgenden Ausführungsbeispiel verwendeten Protokolle entsprechend den bekannten Internetstandards RFC2327, RFC2543 und RFC3261 der IETS (Internet Engineering Task Force), siehe http://ietf.org/rfc.html. Wie bereits erwähnt ist die Erfindung auch auf Basis anderer digitaler, paketbasierter Übertragungsprotokolle realisierbar. Als Kommunikationsgeräte KB und/oder KA können Handys, ISDN-Telefone und auch SIP-Software-Clients benutzt werden. Zur technischen Realisierung von VSec bietet sich ein Proxy zwischen KA und dem Internet an, etwa unter Benutzung eines eingebetteten PCs mit mehreren Netzwerkkarten. Dies unterstützt von vorneherein mehrere Clients, die auch mehrere parallele Anrufe durchführen können. VSec kann als ausgehender Proxyserver (outgoing proxy) implementiert werden, der den ursprünglichen „outgoing proxy" in der Konfiguration von Kommuni-

kationsgerät KA ersetzt. Genauso gut könnte der Proxy bei KB oder irgendeinem dazwischen liegenden Knoten angesiedelt sein, sofern dieser alle Kommunikation durchleitet. Der Proxy modifiziert RTP-Ports und IP-Adressen, die in den SIP-Paketen enthalten sind, um sie auf sich selbst umzuleiten und leitet sie dann an den ursprünglichen Empfänger weiter.

[0059] Für die Komponente Arc kann z.B. ein klassischer PC oder Server benutzt werden, der mit der dritten Netzwerkkarte von VSec verbunden ist. Beide kommunizieren über einen zuverlässigen Transmission control protocol TCP-Kanal (für Vertraulichkeit kann z.B. das Transport Layer Security TLS-Protokoll benutzt werden).

[0060] RTP-Pakete werden in Intervalle gruppiert, wobei jedes Intervall gesichert, z.B. digital signiert, und auf Arc gespeichert wird. Jedes Intervall enthält etwa eine Sekunde an RTP-Paketen. Im Beispiel eines zweiseitigen VoIP-Gesprächs existierten effektiv zwei Intervalle pro Sekunde, eins für jeden Kanal bzw. RTP-Strom. Die Dauer eines Intervalls ist einer der Haupt-Konfigurationsparameter, der justiert werden kann. Eine Sekunde stellt sich Erfahrungsgemäß als geeignet heraus, um einerseits ein hohes Sicherheitsniveau für den Kontext des Gesprächs im Hinblick auf Verständlichkeit zu bieten. Andererseits hält diese Wahl den Bedarf an Rechenzeit bei weitem niedrig genug für z.B. einen x86-Prozessor und bietet auch ein gutes Verhältnis zwischen Nutzdaten und Speicher-Overhead (z.B. 400 Bytes für Public Key Cryptography Standards PKCS#7 Signaturen die keine Zertifikatskette speichern).

[0061] VSec besitzt nun ein Zertifikat, beispielsweise ein X.509-Zertifikat, zusammen mit dem zugehörigen privaten Schlüssel beispielsweise ein aus der Stand der Technik bekannten RSR-Schlüssel, benannt nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman) um mit Hilfe von asymmetrischer Kryptografie alle Intervalle zu signieren, inklusive der speziellen Start- und End-Intervalle, die zusätzliche Metadaten enthalten. Das Zertifikat, das VSec besitzt, wird in diesem Ausführungsbeispiel nicht nur benutzt, um die Inhalte des Anrufs für das endgültige Archivieren und spätere Überprüfungen zu sichern, sondern auch um VSec gegenüber Arc zu authentifizieren: Intervalle werden nach Fertigstellung direkt an Arc übermittelt, wo dann verschiedene Tests (unter anderem das Überprüfen der Signatur) auf das Intervall angewendet werden und es dann als Segment in eine offene Datei geschrieben wird.

Ausführbare Tests sind insbesondere:

[0062] CHK1 Prüfen, ob das erste Intervall, das so genannte Start-Intervall in den Metadaten ordnungsgemäß von dem externen Zeitstempeldienst T1 signiert wurde. Insbesondere vergleicht Arc die Zeit, d.h. seine lokale Systemzeit, mit der, die von VSec im Intervall gespeichert wurde, um VSec daran zu hindern, die Anruf-Zeit nach vorne zu datieren. Dies kann unabhängig von der Prüfung der von T1 angebrachten Zeitstempel geschehen. Weiterhin kann die T1-Zeitstempelzeit mit der lokalen Zeit von Arc und mit der von VSec in den Intervallen aufgezeichneten auf Diskrepanzen überprüft werden. So wird der Zeitraum beschränkt, in dem die zpdK-Daten unter alleiniger Verfügung von VSec stehen und evtl. von VSec verfälscht werden können.

[0063] Wenn ein weiterer Beweis über den Kommunikationszeitpunkt durch eine dritte Partei (z.B. ein Einzelverbindungsnachweis eines Telekommunikationsdiensteanbieters) existiert, kann dieser ebenfalls mit dem ersten Zeitstempel verglichen werden.

[0064] CHK2 Überprüfung der Sicherung des Intervalls, z.B. der PKCS#7 Signatur. Dies authentifiziert VSec gegenüber Arc und stellt sicher, dass keine andere Person Intervalle an Arc übermitteln kann. Arc kennt zwar nicht den privaten Schlüssel, der nur VSec bekannt ist, kann ihn aber gegen das Zertifikat und einen Vertrauensanker prüfen.

[0065] CHK3 Überprüfung der Intervall-Verkettung. Arc berechnet (aus den vollständigen Intervalldaten des vorhergehenden Intervalls) den zur Verkettung mit dem vorhergehenden Intervall benutzten Sicherungswert, z.B. einen aus dem Stand der Technik bekannten Secure Hash Algorithm SHA1- oder SHA-256-Hash-Wert, oder ähnliches und vergleicht ihn mit dem eingebetteten Sicherungswert im aktuellen Intervall. Wenn sie nicht übereinstimmen, wurde die Kette unterbrochen und die Kommunikation wird abgebrochen. Dies stellt eine analoge Ausführung der Sicherheitspolitik 4 aus Abschnitt 2.4.1 dar.

[0066] CHK4 Überprüfung des Paketverlusts durch Prüfen der absoluten Sequenznummern in der Intervall-Datenstruktur. Wenn der Paketverlust oberhalb der Quality of Service QoS-Grenze liegt, wird das Archivieren von Arc abgebrochen und der Anruf von VSec unterbrochen, indem nach dem Einspeisen eines „BYE"-Kommandos das Weiterleiten von SIP und RTP eingestellt wird. Man kann zum Beispiel 1% als Paketverlust-Grenze wählen. Dadurch wird eine gute Verstehbarkeit sichergestellt.

[0067] CHK5 Überprüfung der Zeit, die von VSec in den Intervallen eingebettet wurde, ob sie nicht mehr als die doppelte Intervalldauer von der internen Uhrzeit von Arc abweicht. Die internen Uhren können zum Beispiel mit NTP synchronisiert werden. Dies sollte in einem Produktionssystem durch eine sichere, vertrauenswürdige Zeitquelle ersetzt werden.

[0068] CHK6 Überprüfen der zeitlichen Integrität der RTP-Pakete, also insbesondere, ob die Zeitstempel und Sequenznummern, die im RTP-Protokoll übertragen werden und von Überläufen und Überlappungen geprägt sind, konsistent zur im Intervall gespeicherten Zeit sind.

[0069] Auf diese Weise wird die gesamte Konversation kontinuierlich und sicher von VSec zu Arc gestreamt und VSec muss nie mehr als 2 Sekunden an RTP-Paketen pro gleichzeitigem Anruf im Speicher behalten (insbesondere ist eine Festplatte in VSec im Prinzip nicht notwendig). Außerdem muss VSec nur etwa 2 (RSA-)Signatur-Operationen pro Sekunde durchführen.

[0070] Das Format, mit dem der Anruf von VSec zu Arc gesandt wird, besteht aus Intervallen, einschließlich einem speziellen anfänglichem Intervall mit Metadaten, einem abschließendem Intervall das den Grund der Gesprächsabbruch enthält und verschiedenen Intervallen mit Sprachdaten (Start- und End-Intervall enthalten keine Sprachdaten). Das Datenformat und die Verkettung der Intervalle sind in Fig. 3 gezeigt. Jedes Intervall kommt entweder vom RTP-Kanal von A zu B oder der entgegengesetzten Richtung. Jedes Intervall ist in diesem Beispiel in einen PKCS#7-„signed envelope"-Container eingebettet. Nur der erste PKCS#7-„signed envelope"-Kontainer enthält die gesamte Zertifikatskette bis zur, aber nicht einschließlich der Zertifikatswurzel, während alle anderen Container diese redundanten Informationen nicht enthalten müssen. Das erste Intervall ist außerdem zusätzlich in eine Signatur des Zeitstempeldienstes T1 eingebettet. Arc speichert einfach jedes Intervall (zusammen mit seiner Signatur) auf z.B. seine Festplatte, nachdem die beschriebenen Tests darauf angewendet wurden.

[0071] Der signierte und mit einem Zeitstempel versehene Inhalt des ersten Intervalls besteht aus:

- Einem zufälligen Nonce. Dies verhindert einen Wiedereinspielungs- und einen Verdopplungsangriff, siehe Abschnitt 3.4
- Datum und Uhrzeit des Anrufs
- Absender- und Ziel-SIP-URL des Anrufers und Angerufenen
- Die Zuordnung der RTP-„Payload-Types" zu den tatsächlich verwendeten Medienformaten und Codecs. Diese Information ist in den Session Description Protocol (SDP)-Daten von z.B. dem INVITE-Befehl der SIP-Signalisierung enthalten. Ohne diese Information wären die Codecs für die Payload-Typen im dynamischen Bereich von 96–127 später nicht bekannt, wenn der archivierte Anruf abgespielt wird. Als Variante ist es auch möglich, dass die Implementierung die SDP-Aushandlung so modifiziert, dass nur bestimmte Codecs (bei denen es anzunehmen ist, dass sie später noch abspielbar sind, z.B. keine properitären Codecs) erlaubt sind.

[0072] Der signierte Inhalt des letzten Intervalls besteht aus:
Dem Hash des vorletzten Intervalls, um die kryptografische Kette abzuschließen.

- Einem Flag, dass dies das letzte Intervall des archivierten Anrufs ist
- Dem Grund für den Abbruch des Gesprächs: Protokoll- oder Netzwerkfehler, normales Auflegen des Hörers durch A oder B, Verstoß gegen die Paketverlust QoS-Grenze oder Manipulationsversuch.

[0073] Die anderen Intervalle enthalten die eigentlichen Sprachdaten und bestehen aus:

- Einem Hash über das komplette, signierte (und – im Fall von Intervall Nr. 2 – mit einem Zeitstempel versehenen) Intervall, das diesem Intervall vorausging.
- Datum und Uhrzeit dieses Intervalls
- Richtung/Kanal dieses Intervalls. In der Implementierung für Duplex-Kommunikation zwischen nur zwei Parteien kann dies die Richtung A nach B oder die Gegenrichtung sein.
- Einer Liste der absoluten Sequenznummern der enthaltenen RTP-Pakete
- Den kompletten RTP-Paketen, auf die diese Liste verweist, inkl. ihrer Payload-Typen und den abgeschnittenen Zeitstempeln und Sequenznummern.

[0074] Alle Intervalle zusammen bilden eine kryptografische Kette vom ersten bis zum letzten Intervall. Intervalle beider Richtungen (bzw. Kanälen der Duplex-Kommunikation) sind miteinander verwebt. Nach zwei Intervallen einer Richtung muss ein Intervall der anderen Richtung kommen und Datum und Uhrzeit müssen zueinander passen. Andernfalls muss Arc (oder jeder andere Überprüfer des archivierten Anrufs) die Datei ablehnen, ganz genauso wie wenn ein Hash oder eine Signatur ungültig wären.

[0075] VSec enthält eine Komponente, die eingehende Pakete sortiert und einen Schutz gegen Wiedereinspielung enthält, indem doppelte Pakete entfernt werden. Dies ist z.B. durch ein 32-Bit Schieberegister zu realisieren. Solche Komponenten zum Schutz vor Wiedereinspielungen gehören zu den Standard-Techniken im Design sicherer Kommunikationsprotokolle. Da RTP-Pakete nur 16-Bit-Sequenznummern enthalten (für die sogar empfohlen wird, dass das erste Paket nicht mit 0 oder 1 beginnt, sondern mit einem Zufallswert, um symmetrische Verschlüsselung zu unterstützen) und auch nur 32-Bit Zeitstempel (die ebenfalls mit einem zufälligen Wert starten, überlaufen können und nichts mit der absoluten Zeit zu tun haben) hilft diese Komponente auch dabei, absolute Sequenznummern zu erzeugen, die mit 0 beginnen und nicht überlaufen. Außerdem prüft

sie die Systemzeit gegen die Zeitstempel der Pakete auf Konsistenz. Wenn irgendeine dieser Prüfbedingungen verletzt wird, wird der Anruf abgebrochen. Wenn VSec dies nicht erkennen sollte (z.B. auf Grund einer Manipulation), dann würde Arc das Archivieren abbrechen, da Arc die gleichen Tests durchführt.

3.4 Sicherheitsanalyse

[0076] Die angestrebte Sicherheit des gezeigten zpdK-Archivs ist die eines analogen (Band-)Archivs für analog geführte Telefongespräche. Obwohl das Fälschen natürlicher Sprache durch Synthese allgemein als schwierig gilt, ist es einem Angreifer, der über ausreichende Ressourcen verfügt, prinzipiell möglich komplett gefälschte Telefonate in das Archiv einzuspielen, z.B. von der mit (**2a**) markierten Position in Fig. 2. Solche Angriffe können häufig durch Absicherung von Kommunikationskanälen auf der Transportebene unterdrückt werden und werden hier nicht betrachtet.

[0077] Gemäß den Betrachtungen in Abschnitt 2.4.2 bietet die Umsetzung der Sicherheitspolitik **4**. aus Abschnitt 2.4.1, d.h. Abbruch bei Unterlauf des Kanalqualitäts-Grenzwerts, vorteilhafte Sicherheitseigenschaften. Das gezielte Unkenntlichmachen oder Löschen von Abschnitten in der Mitte eines Gesprächs könnte einem Angreifer sonst die aufgezeigten semantischen Manipulationsmöglichkeiten eröffnen, die zu von ihm absichtlich herbeigeführten Fehlinterpretationen führen können. Dieser Aspekt erlangt besondere Bedeutung für die Beweiskraft über längerer Zeiträume archivierter Gespräche, bei denen die ursprünglichen Sprecher nicht mehr für die Beweisführung zur Verfügung stehen, d.h. befragt werden können.

[0078] Im Folgenden wird gezeigt, welchen Angriffen das vorgestellte sichere zpdK-Archiv zu widerstehen vermag. Die Analyse richtet sich dabei nach der Position eines hypothetischen Angreifers im System, entspreched den nummerierten Positionen in Fig. 2. Die informatorischen Schutzziele, die unter Angriff stehen, werden dabei im Einzelfall genannt.

[0079] (**1**) Man-in-the-middle. Ein Angreifer der die Kommunikation zwischen VSec und Arc abfangen und manipulieren kann (der also etwa eine angelegte Sicherung auf Transportebene gebrochen hat), stellt die größte anzunehmende Bedrohung dar. Für ihn bestehen zwei grundsätzliche Möglichkeiten, gefälschte Gespräche in Arc einzuspielen. Entweder unterbricht er eine andauernde zpdK-Archivierung, etwa nach Intervall N, und setzt sie mit eigens gefälschten Intervallen N+1, N+2, ... fort. Oder aber er initiiert eine eigene zpdK Archivierung und übernimmt die Rolle von VSec selbst. Diese Angriffe bedrohen die Kohäsion eines Gesprächs beziehungsweise die Integrität des Archivs. Spezifische Gegenmaßnahmen sind im vorgestellten Archiv-Konzept bereits beinhaltet oder als Möglichkeit der technischen Ausführung angelegt:
G1.1 Die Verkettung der Intervalle mittels eines kryptografischen Geheimnisses gemäß Abschnitt 2.2 verhindert die erste Angriffsvariante, da (**1**) die Kette der Intervalle nicht eigenständig fortsetzen kann, wenn er dieses Geheimnis nicht kennt. Damit (**1**) bei diesem Angriffsversuch erkannt werden kann, sollte die Benutzung des korrekten Geheimnisses durch VSec auf Seiten von Arc verifizierbar sein. Hierfür bieten sich verschiedene symmetrische und asymmetrische kryptografische Verfahren an.
G1.2 Die Sicherung des Start-Intervalls in geeigneter, nur VSec und Arc bekannter Weise unterdrückt die zweite Angriffsvariante. Zur Erhöhung der Sicherheit können hier zum Beispiel das aus dem Stand der Technik bekannte Diffie-Hellman Protokoll zur Aushandlung eines geheimen Schlüssels, oder wie im technischen Ausführungsbeispiel in Abschnitt 3.3., digitale Signaturen mittels asymmetrischer Kryptoverfahren zum Einsatz kommen.

[0080] Die Gegenmaßnahmen G1.1 und G1.2 sind bereits im Konzept des Archivs angelegt. Die weiteren nun folgenden Gegenmaßnahmen sind von ihnen abhängig und dienen einer weiteren, graduellen Erhöhung der Sicherheit des Archivsystems.

[0081] (**2**) Fälschung durch Wiedereinspielung. In der Position (**2**) kann ein Angreifer gegenüber VSec eine zpdK simulieren. Eine Möglichkeit für (**2**), die Integrität des Archivs zu kompromittieren ist, einen kurzen Abschnitt vom Anfang eines echten Gesprächs zwischen A und B aufzuzeichnen, zu einem späteren Zeitpunkt wiedereinzuspielen, und nach eigenem Gutdünken fortzusetzen (synthetisiert, zusammen geschnitten, oder sogar in Komplizenschaft mit A und/oder B). Es ist dann später leichter abzustreiten, das die ursprüngliche, authentische zpdK stattgefunden hat, da Arc nun zwei archivierte Gespräche mit sehr ähnlichen oder sogar bitweise identischen Anfängen enthält.

[0082] (**2a**) Fälschung durch Wiedereinspielung mit Kontrolle der zpdK-Quelle. Die Bedrohung durch Wiedereinspielungen ist noch größer von dieser Position aus. Denn der Angriff von (**2**) aus ist technisch durchaus schwierig, da (**2**) wegen der Unvollkommenheit z.B. des VoIP-Kanals nicht genau weiß, welche Pakete des Original-Gesprächsanfangs bei VSec ankamen. Abhängig von der Intervalllänge kann dies schon für die ersten paar Intervalle zu bemerkbaren Diskrepanzen führen, die (**2**) verraten. Mögliche Gegenmaßnahmen gegen eine Wiedereinspielung von (**2a**) aus sind G2.1 Ausnutzung von Zufälligkeiten von Voice over IP, insbesondere Paket-Verlust. Dies macht (**2**) wie gesagt bemerkbar, wenn die Intervalllänge hinreichend groß ist, aller-

dings nur mit einer gewissen Wahrscheinlichkeit, die z.B. von der Paket-Verlustrate abhängt.

[0083] G2.2 Eine Zufallszahl hoher Qualität in das Start-Intervall einzubauen ist eine erheblich stärkere Gegenmaßnahme und verhindert auch effektiv den Angriff von (**2a**). In der technischen Ausführung in Abschnitt 3.3 fügt VSec insbesondere eine zufällige Nonce ein.

[0084] Was mit einem Gespräch geschieht, das als Artefakt eines Wiedereinspielungs-Angriffs erkannt wurde, insbesondere ob es im Archiv verbleiben oder nur markiert werden soll, bestimmt sich je nach Anwendungsfall.

[0085] (**3**) Kompromittiertes Geheimnis von VSec. Ein Angreifer, der VSecs Geheimnis zur Sicherung der Intervallkette und ggf. zur Authentisierung gegenüber Arc kennt, erscheint für Arc wie VSec selbst. Er ist daher in der Lage wie (**1**), nur mit erhöhter Wirksamkeit, gefälschte Gespräche in Arc einzuführen. Dennoch gibt es zwei mögliche Gegenmaßnahmen.

[0086] G3.1 Als interne Maßnahme kann VSec Einmal-Geheimnisse benutzen, die aus einem Master-Geheimnis abgeleitet werden und sich für jedes Gespräch unterscheiden. Das Master-Geheimnis müsste dann erheblich besser als die Einmal-Geheimnisse gegen Offenbarung geschützt sein.

[0087] G3.2 Eine externe Quelle für zusätzliches Vertrauen kann zur Sicherung jedes einzelnen Gesprächs miteinbezogen werden. Im Ausführungsbeispiel ist hier der Zeitstempeldienst eingeführt worden, der das Start-Intervall jedes Gesprächs mit einem signierten Zeitstempel versieht. G3.2 erhöht zusätzlich die Sicherheit bezüglich Wiedereinspielungsangriffen (**2**), bzw. (**2a**).

[0088] (**4**) Fälschungen durch den Archivar. Diesen wird durch Eigenschaften der Architektur wie in **Fig. 2** gezeigt vorgebeugt.

[0089] G4.1 Die Teilung von Aufgaben und Verantwortlichkeiten zwischen VSec und Arc macht es Arc schwer, gesicherte zpdK zu fälschen und zu behaupten, sie stamme von VSec. Dies gilt insbesondere stets in der asymmetrischen Situation in der Arc das Geheimnis von VSec nicht kennt, aber verifizieren kann (wie z.B. bei asymmetrischer Kryptografie). Selbst wenn (**4**) sich zudem in der Position von (**3**) befindet und VSecs Geheimnis kennt, wirkt noch immer G3.2 und hindert ihn daran, Gespräche zu erzeugen, die wie solche von VSec „aussehen".

[0090] G4.2 Als grundsätzliches Problem der Langzeitarchivierung digitaler Daten verbleibt die Hoheit von Arc über diese. Mit hinreichend Zeit und Rechenleistung versehen kann Arc oder jemand mit Zugriff auf Arc die archivierten Gespräche manipulieren. Eine Methode, die gemeinhin als wirksam gegen solche Bedrohungen angesehen wird, ist das periodische Auffrischen von Zeitstempeln über die archivierten Daten, z.B. unter Zuhilfenahme eines weiteren Zeitstempeldienstes T2. Effizient wird dies durch so genannte Hash-Bäume realisiert.

[0091] Weitere Angriffe können durch ein Zusammenspiel der Angreifer (**1**)–(**4**) versucht werden, sind aber alle durch die gezeigten Gegenmaßnahmen ausgeschlossen. Zum Beispiel kann (**1**) in Kombination mit (**2a**) versuchen einen zurückdatierten Anruf in Arc einzuspielen. Er würde dazu Anrufe zu von ihm gewählten Zeitpunkten in VSec einspielen (**2a**), die von VSec abgehenden initialen Teile dieser Anrufe einschließlich der Zeitstempel von T1 einsammeln (**1**) und die Übertragung an Arc unterdrücken. Später würde er den Anruf, den er zurückdatieren möchte, von (**2a**) aus einspielen, wobei er von (**1**) aus das initiale Intervall mit einem „gestohlenen" seiner Wahl, d.h. mit dem ihm genehmen Zeitstempel, ersetzt. Auch dieser Angriff schlägt jedoch fehl aufgrund der Verkettung der Intervalle und der Eindeutigkeit der initialen Intervalle die zum Beispiel durch zufällige Noncen erzwungen wird. Das heißt, es greifen hier G2.2, im Zusammenhang mit G1.1 und G1.2.

4. TA 3) Authentisierung von Kommunikationspartnern

[0092] Unerwünschte Anrufe durch verschiedenste Organisationen oder Personen nehmen verstärkt zu. In diesem Bereich haben sich die Begriffe SPIT (SPam over Internet Telephony) und Phishing (erlangen von Informationen durch Vortäuschen von Identitäten) etabliert. Entsprechende Organisationen verwenden zunehmend internetbasierte zpdK, da diese den Betreibern eine erhöhte Anonymität durch frei wählbare Anruferidentifikation und Kostenreduktionen ermöglichen. Es droht besonders durch automatisierte Anrufe, dass sich der Benutzer einer ähnlichen Flut von ungewünschten Anrufen ausgesetzt sieht, wie dies bereits im Bereich der elektronischen Post der Fall ist.

[0093] Diesem kann im technischen Bereich hauptsächlich durch eine hinreichende Authentisierung der Kommunikationspartner begegnet werden. SIP beispielsweise bietet hier eine anfängliche Authentisierung, welche auf einem shared secret (Passwort) und einem Frage/Antwort-Prinzip (challange/response) beruht (siehe RFC2617) oder lediglich die bekannte http-Basic Authentisierung (siehe RFC 2543). Nachdem die Authentisierung durchgeführt ist, wird dem zpdK-Datenstrom vertraut. Eine Validierung des Ursprungs wird danach nicht durchgeführt, so dass die Möglichkeit besteht, hier einen zweiten Datenstrom einzuschleusen, welcher dem entsprechenden Kommunikationspartner wiedergegeben wird. RTP bietet

hier die Möglichkeit durch die Verwendung von SRTP einen Schutz der Vertraulichkeit der Daten zu erreichen. Außerdem stellt SRTP auf Basis eines geheimem Sitzungsschlüssels sowie eines HMAC Authentizität bereit. Durch den Einsatz eines symmetrischen Sitzungsschlüssels, dessen sichere, authentische Übertragung schwierig ist, kann SRTP die Authentizität in vielen Szenarien nicht für die gesamte Dauer des Gesprächs sichern. Hierzu ist auf jeden Fall eine Sicherung der Kohäsion nötig, so dass ein Gesprächspartner sicher sein kann, während der gesamten Dauer eines Gesprächs, denselben Partner auf der Gegenseite zu haben.

4.1 Methode und Ausführung

[0094] Die hier vorgestellte Methode kann auf bestehende Methoden wie z.B. SRTP aufsetzen und die in Abschnitt 1.2 beschriebenen Eigenschaften der Integrität und Kohäsion sichern. Hierzu wird eine Authentisierung am Anfang der Kommunikation durchgeführt, welche sich auf eine oder mehrere der bekannten Klassen von Authetisierungstoken Besitz, Wissen oder Sein stützen kann. Diese Information wird in das Start-Intervall integriert. Hierdurch wird die Authentisierung Bestandteil der Kommunikation. Dieses Start-Intervall wird als Basis für die aus Abschnitt 2 bekannte Intervall-Kette verwendet. Der Empfänger kann die in Abschnitt 3.2 beschrieben Prüfungen durchführen und hierdurch feststellen, dass der Datenstrom der zpdK auf dem Start-Intervall beruht.

[0095] Die Integration kann an verschiedenen Stellen der zpdK erfolgen. Zumeist wird eine Integration in das Kommunikationsendgerät erfolgen, welches beispielsweise unter der direkten Kontrolle des Besitzers ist. In einem organisationsweiten Einsatz bietet sich eine Integration in die Kommunikationsgeräte (z.B. Telefonanlagen) an, welche diese Funktionalität dann zentral den Benutzern anbieten.

[0096] Es ist hier zu beachten, dass für die prinzipielle Methode zur Authentisierung keine Archivierung des Datenstroms gefordert wird. Die Authentizität des Kommunikationspartners kann durch eine permanente Signalisierung des empfangenden Kommunikationsendgerätes gegenüber dem Benutzer erfolgen, nachdem dieser sich vor oder während der Kommunikation von der Identität des Kommunikationspartners überzeugt hat. Diese Signalisierung kann in verschiedener Ausführung geschehen, da dies vom Anwendungsfall abhängig ist. Eine mögliche Signalisierung kann durch das Kommunikationsendgerät erfolgen, welches synthetisierte Multimediadaten in den Kanal einblendet (z.B. durch eine Sprachmeldung „Sie sind mit dem authentisierten Anschluss von Herrn X verbunden" oder durch Anzeige eines Bildes der Person). Dieser Weg kann auch erfolgen, falls sich die Funktionalität z.B. in einem Kommunikationsvermittlungsgerät befindet. Es kann auch in dem Gerät in Form einer einfachen visuellen Signalisierung (z.B. grüne Lampe) erfolgen.

[0097] Im Fall eines Abbruchs der Intervall-Kette, wie in Abschnitt 2.4.2 beschrieben, können die Politiken aus Abschnitt 2.4.1 durchgeführt werden. Hierbei ist der jeweilige Kontext der Verwendung der Methode zu beachten und eine angemessene Politik zu wählen. Falls eine permanente Signalisierung durch das Kommunikationsendgerät erfolgt, muss diese entsprechend den Politiken den Abbruch signalisieren. Es ist wünschenswert, dass dies für den Benutzer deutlich erkennbar ist.

[0098] Bis hierher ist die Methode zur Lösung von TA 3 ähnlich der von TA 2, in der VSec einen in analoger Weise gesicherten zpdK-Strom an die Archivierungs-Komponente sendet. Aufgrund der nun bidirektionalen Kommunikation zwischen A und B, ohne zwischen liegende Sicherungskomponente, ist nun aber eine gesonderte Behandlung von Paketverlusten nötig.

[0099] Zur Beschreibung der Methode und als technisches Ausführungsbeispiel wird hier das Szenario auf den Fall reduziert das eine Person A einer Person B seine Identität mitteilen möchte. Die Methode kann aber auch auf komplexere Szenarien angewendet werden, die mehrere Kommunikationspartner involvieren. KA und KB sammeln permanent alle Pakete in einem kleinen Zwischenspeicher, wie dies in **Fig. 4** dargestellt wird. Sobald KB auf bestimmte Weise angeregt wird, sendet KB eine Liste von Paketsequenznummern von gesammelten Paketen aus dem aktuellen Intervall an KA. Die notwendige Anregung kann zeitgesteuert oder paketorientiert sein oder könnte auch durch eine explizite Anfrage von KA ausgelöst werden.

[0100] KA berechnet die Sicherungswerte der in einem Intervall gesammelten Pakete und erzeugt und sichert die Intervalldaten. Die Sicherung muss in jedem Intervall die Authentisierung von A durch B ermöglichen, was den Kern der kontinuierlichen Authentisierungsmethode ausmacht. Wie in **Fig. 4** gezeigt beinhalten die Intervalldaten insbesondere einen Verkettungs-Wert V(vorhergehendes Intervall), z.B. einen Hash-Wert, der jeweils vorherigen Intervalldaten wodurch Verkettung erreicht wird. Die gesicherten Hash-Werte h(Paket) werden dann an B übertragen. B kann anhand dieser Daten die Hash-Werte mit denen der von ihm tatsächlich empfangenen Pakete vergleichen und die Sicherung der Intervalldaten überprüfen.

[0101] Das zuvor beschriebene Start-Intervall unterscheidet sich dann dadurch von den weiteren Intervallen, dass letztere keine Daten des Authentisierungstokens mehr enthalten müssen. Konkrete Me-

thoden zur Sicherung sind vielfältig, zum Beispiel kann das Start Intervall von A digital signiert werden und zusätzlich ein digitales Zertifikat enthalten, dass A als Besitzer des privaten Signaturschlüssels ausweist, während weitere Intervalle nur noch von A digital signiert werden. Im Unterschied zur weiter unten in Abschnitt 5 beschriebenen Methode zur kompletten Signierung eines Gesprächs durch A wird aber immer noch nicht die Kommunikationsrichtung von B nach A gesichert. Digitale Signaturen sind zur Authentisierung wie hier beschrieben nicht die einzige technische Möglichkeit. Zum Beispiel könnten A und B auch mittels des bekannten Diffie-Hellman Verfahrens einen geheimen, symmetrischen Schlüssel vereinbaren, der zur Sicherung der Intervalle nach dem Start-Intervall verwendet wird.

[0102] Durch die Rückmeldung von KB wird sichergestellt, dass KA lediglich übermittelte Pakete sichert. Nicht bestätigte Pakete werden verworfen. Des Weiteren erhält KA einen Wert für die Kanalqualität, der im Rahmen von sicherheitsrelevanten Politiken ausgewertet werden kann. Dies sind zwei grundlegende Vorteile der Authentisierung mit Rückmeldung durch B gegenüber einer einfachen Variante, bei der KA einfach alle gesendeten Pakete in Intervallen sichert. Die Rückmeldung bietet A zusätzliche Sicherheit in dem Fall, dass B die Kommunikation etwa ohne Wissen von A aufzeichnet. Mit Rückmeldung ist A dennoch sicher, dass er nur von ihm ausgehende zpdK authentisiert, die bei B angekommen ist. B erreicht nichts dadurch, z.B. mehr Pakete als empfangen zu melden, als er wirklich erhalten hat, da er damit höchstens Authentisierungsdaten für Sprachdaten erhält, die er später nicht vorzeigen kann.

[0103] Die Bildung der Intervall-Kette entspricht dem Verfahren 2. aus Abschnitt 2.3 zur Behandlung von Paketverlusten. Die anderen Varianten 1., 3., und 4. können alternativ angewendet werden. In **Fig. 4** werden lediglich Audiodaten betrachtet. Es ist aber problemlos möglich auch andere Kommunikationsdaten zu erfassen, da das vorgestellte Verfahren transparent gegenüber den zu sichernden Daten ist.

[0104] Bei der Übertragung der Paketsequenznummern von B zu A ist zu beachten, dass die Übermittlung gegen Datenverlust zu sichern ist. B sollte entweder ein Protokoll wie z.B. TCP verwenden, welches die Übertragung sichert oder auf eine andere Art eine Bestätigung erhalten über den Empfang des Paketes. Eine Erweiterung der Datenstruktur um Integritätssichernde Daten wie z.B. ein Cyclic Redundancy Check (CRC) oder HMAC kann je nach verwendetem unterliegendem Transportprotokoll sinnvoll sein. Falls kein sicherndes Transportprotokoll zur Anwendung kommt, muss dies durch ein eigenes Protokoll nachgebildet werden. Hierzu werden Empfangsbestätigungen und Zeitgrenzen verwendet, welche ein erneutes Versenden anstoßen. Als Empfangsbestätigung kann auch das durch KA erzeugte Intervalldatenpaket verwendet werden.

[0105] Die Anforderung einer gesicherten Übertragung gilt ebenso für die gesicherten Intervalldaten (von A nach B). Wenn B das Paket erhält, muss es den Empfang gegenüber KA quittieren und damit die Intervallnummer, welche eine monoton steigende, eindeutige Nummer für die Intervallpakete ist, übertragen. Hiermit wird sichergestellt, das KB die gesicherten Intervalldaten erhalten hat. Dies ist nicht selbstverständlich, da der Übertragungskanal, wie etwa bei User Datagram Protocol (UDP) der Fall, verlustbehaftet sein kann. Falls nach einer bestimmten Zeit diese Quittierung nicht bei KA eintrifft, so ist eine Neuübertragung notwendig.

[0106] Nach der Berechnung der Hash-Werte durch KA (angestoßen durch die übermittelten Paketnummern von KB) können alle gesammelten Pakete des Intervalls gelöscht werden, da im Fall eines Übertragungsfehlers lediglich die Intervalldaten neu übertragen werden müssen, nicht aber die zpdK-Datenpakete.

5. TA 4) Signatur

[0107] Aus dem Bereich der Geschäftkorrespondenz ergeben sich zwei unterschiedliche Fälle, in denen Nichtabstreitbarkeit verlangt wird. Im ersten Fall gibt eine Partei eine einseitige, Erklärung ab (z.B. ein Angebot), welches ab diesem Zeitpunkt bindend ist, was zum Beispiel durch eine Signatur erreicht wird. Der zweite Fall behandelt mehrseitige Erklärungen (z.B. Verträge), die durch mehrere Parteien unterzeichnet werden müssen und dann auch für diese bindend sind. Bei digitalen Signaturen gibt es hier die Möglichkeit mehrere Signaturen an ein Dokument anzubringen, entweder parallel, oder ineinander verschachtelt.

[0108] In einem vereinfachten Szenario in welchem zur besseren Illustration lediglich die Parteien A und B agieren, entspricht der erste Fall einer Absicherung der Kommunikation von A nach B, was prinzipiell der in Abschnitt 4 vorgestellten Methode ähnelt. Es müssen aber insbesondere Methoden zur Aufzeichnung der zpdK bei B und eine vollständige Sicherung beider Richtungen des zpdK-Stroms ergänzt werden. Denn zur Wahrung des Gesprächs- oder Verhandlungs-Kontextes also der Kohäsion, sind in diesem Fall die Äußerungen beider Gesprächspartner wesentlich. Nur sie zusammen (und im richtigen zeitlichen Zusammenhang) ergeben das zpdK-Analogon zum digital zu signierenden Dokument.

[0109] Der zweite Fall kann durch zwei unterschiedliche Ansätze gelöst werden. Der naive Ansatz führt Fall eins, d.h. eine Signatur der zpdK von A für B bzw. von B für A für jeden Kommunikationspartner durch.

So entstehen auf beiden Seiten signierte Datensätze, die zwar beide für sich genommen gültig, aber nicht bitweise identisch sind, was vorteilhaft wäre. Außerdem ist jeder Datensatz nur von der jeweiligen Seite signiert. Erst wenn beide vollständig und gleichzeitig vorliegen erhalten sie einen mehrseitigen Nichtabstreitbarkeitscharakter. Ein solcher Ansatz ist ineffizient und bedarf zum späteren Nachweis insbesondere jeweils eine Überprüfung der (wenigstens zwei) Datensätze durch „Ohrenschein" oder Inhaltsvergleich.

[0110] Daher ist es wünschenswert eine einheitliche Datenstruktur analog zu einem digitalen Dokument mit mehreren elektronischen Signaturen zu erzeugen, welche bei allen Parteien entsteht und durch alle Parteien bestätigt wird. So ist jeder Kommunikationspartner im Besitz eines Dokumentes, welches eine Kommunikation nichtabstreitbar dokumentiert. Diese einheitliche Datenstruktur erfüllt die Forderung nach Kohäsion, welche in Abschnitt 1.2 beschrieben ist.

5.1 Signaturszenario und Basiskonzept

[0111] Fig. 5 zeigt das bereits vorgestellte vereinfachte Szenario in dem eine zweiseitige, interaktive Kommunikation zwischen den Parteien A und B stattfindet, die hier beispielsweise über Vermittlungsgeräte KA und KB läuft. A möchte den Gesprächsinhalt unabstreitbar an B übertragen (Fall 1 in der Einleitung zu Abschnitt 5). Dies wird im weiteren Verlauf als zpdK-Willenserklärung bezeichnet und beinhaltet eine explizite Willenserklärung durch A, dass der Gesprächsinhalt durch ihn selbst in Zukunft nichtabstreitbar ist. Diese neue Bezeichnung dokumentiert insbesondere die Unterscheidung zu elektronischen Signaturen digitaler Dokumente, bei denen es nicht um zeitlichen Bezug und Ablauf eines kontinuierlichen Kommunikationsprozesses geht.

[0112] Zum Zwecke der zpdK-Willenserklärung besitzt A einen dafür bestimmten Token, z.B. ein digitales Zertifikat, welcher von A zur Sicherung der Intervalldaten eingesetzt wird. A signiert die vollständige Kommunikation inklusive aller ein- und ausgehenden Daten. Hierdurch wird das komplette Gespräch durch die Signatur erfasst. B kann die resultierende Datenstruktur in einem sicheren Archiv seiner Wahl aufbewahren. Diese archivierte Version kann B später als Beweis einer dritten Partei vorlegen, dass das Gespräch stattgefunden hatte. Falls B die Datenstruktur löscht, kann A das Gespräch leugnen.

[0113] In der technischen Umsetzung wird in der Regel eine Funktionalität zur Aufzeichnung und Archivierung auf Seiten von B integriert werden. Die Aufzeichnung, die Anforderungen an das Archiv und die Übertragung an das Archiv durch die Aufzeichnungskomponente sind durch die entsprechende Beschreibung in Abschnitt 3 (Archiv) abgedeckt.

[0114] Eine technische Ausführung dieses Szenarios kann auf SIP/RTP basieren. Es ist wiederum anzumerken, dass ebenfalls das Inter-Asterisk-Protokoll (AIX) oder das bekannte H.323 benutzt werden könnten, da die vorgestellte Methode unabhängig vom unterliegenden Protokoll angewendet werden kann. Im Folgenden wird SIP/RTP als durchgängiges Beispiel verwendet. Das Signaturprotokoll erweitert den SIP/RTP Standard in einem kompatiblen Weg um Transportsignaturen und Bestätigungen dieser Signaturen.

[0115] Da das Signieren einzelner Pakete wie gezeigt ineffizient ist, wird Methode 2 aus Abschnitt 2.3 verwendet. Hierdurch werden die Konzepte der Intervalle und Intervalldaten, wie in Abschnitt 2.1 eingeführt, angewendet. Der Begriff der Intervallsignatur beschreibt die Sicherungswerte (siehe Abschnitt 2.1), die benötigt werden die Intervalldaten abzusichern. Sie haben zur Lösung der TA 4 Signaturcharakter und müssen A entsprechend ausweisen, z.B. durch asymmetrische Kryptografie und digitale, Public Key Infrastructure (PKI)-basierte Zertifikate.

[0116] In der Signalisierungsphase des SIP-Protokolls werden die Beschreibung der Anrufparameter inklusive der IP-Adresse, Ports, Multimediacodecs und deren Parameter im SIP Paket (eingebettet in ein SDP-Paket) zum Kommunikationspartner transportiert. Es wird ein ähnlicher Applikations-Datenstrom für den Transport der Signaturdaten verwendet. Dieser ist UDP-basiert und daher nicht als zuverlässig anzusehen, da hier Paketverluste eintreten können. Der Wunsch zur Signalisierung wird durch einen speziellen so genannten k-Wert im SDP-Paket an den Kommunikationspartner signalisiert. Hierfür existieren viele Alternativen. Die genaue Art der Signalisierung ist nicht relevant für die Methode und lediglich exemplarisch.

[0117] Jede Partei sammelt nun Pakete in Intervallen von einstellbarer Länge. Die Intervalllänge kann zeit- oder paketbasiert bestimmt werden. Am Ende eines Intervalls werden die Pakete sortiert anhand ihrer Sequenznummern und ihre Hash-Werte zusammen mit notwendigen Zusatzdaten wie Richtung der Übertragung, Sequenznummer und Zeit in einer Datenstruktur zusammengefasst (Intervalldaten) und dann z.B. durch den RSA-Algorithmus signiert unter Verwendung des Signaturtokens von A. Diese Einheit wird an KB übertragen, welcher diese in Verbindung mit den dazugehörigen Pakten speichert. Es ist zu beachten, dass die eigentlichen zpdK-Daten aufgrund der Methode nicht noch einmal übertragen werden. Dies führt zu einer guten Bandbreiten- und Rechenzeit-Ausnutzung.

[0118] Da signierte Intervalle die geforderte Kohäsion nicht sicherstellen, denn ein Angreifer könnte einzelne Intervalle austauschen, müssen die Pakete un-

tereinander verkettet werden, wie dies in Abschnitt 2.2 beschrieben wird. Hierdurch wird eine Intervall-Kette gebildet, aus der einzelne Intervalle nicht entfernt oder ausgetauscht werden können. Die Signaturkette bricht bereits, wenn ein einzelnes Bit in der Kette oder in den Paketdaten verändert wird. Durch die Wahl von Methode 2 aus Abschnitt 2.3 können bei Bitfehlern in einzelnen Intervallen diese Intervalle lokalisiert werden und unter Umständen eine eingeschränkte, forensische Aussage über die Glaubwürdigkeit der Aufzeichnung gemacht werden.

[0119] Die Signatur erstreckt sich – im Unterschied zum Authentisierungsverfahren aus Abschnitt 4 – auf beide Kanäle der Kommunikation und wird so der bidirektionalen Natur der Kommunikation gerecht. Die Signatur über den Kanal von A nach B entspricht dabei der Methode aus Abschnitt 4.1 in der technischen Ausprägung, die in Fig. 4 gezeigt ist. Die notwendige Signierung der Daten von B nach A unterscheidet sich davon, wie in Fig. 6 zu sehen. Wieder sammeln KA und KB alle Pakete auch dieses Kanals. KA entscheidet, wann ein neues Intervall beginnt. KA nimmt dann die übertragenen und sortierten Pakete von B nach A, erzeugt Hash-Werte über diese und erzeugt ein Datenpaket aus den Hash-Werten und signiert dieses. Dieses Datenpaket entspricht einer Intervallsignatur und wird an den Kommunikationspartner B übertragen, was auf geeignete Weise, etwa durch Quittierung durch KB, abzusichern ist, wie in den letzten drei Absätzen von Abschnitt 4.1 beschrieben. Start- und Endintervalle werden durch KA entsprechend Abschnitt 4.1 gebildet.

[0120] Die beiden Richtungen werden nun miteinander untrennbar verwoben. KA übernimmt hierzu eine Steuerungsfunktion, die auf verschiedene Weisen ausgeführt werden kann. Zum Beispiel könnte KA nach jedem Intervall von A nach B die Erzeugung eines Intervalls von B nach A erzwingen. Dies hätte den Nachteil, dass letzteres Intervall gegebenenfalls keine zpdK-Pakete enthalten würde, wenn KB in der Zwischenzeit nicht sendet. Ein solcher Fall wäre gesondert zu behandeln. Die hier bevorzugte Ausprägung für den Richtungswechsel zwischen Intervallen funktioniert deshalb asynchron. KA führt gleichzeitig zwei Puffer für Sende- und Empfangsrichtung. Je nachdem, ob sein Sendepuffer zuerst voll gelaufen ist, oder ihn zuerst eine Rückmeldung über empfangene Pakete von KB erreicht (siehe Fig. 4) bildet KA ein Intervall der entsprechenden Richtung. Es kann hierbei hilfreich sein, die Intervalllänge dynamisch anzupassen wie es im vorletzten Absatz von Abschnitt 3.1 beschrieben wurde, um Verzögerungen, d.h. ein Hinterherhinken des Bildens und Sicherns von Intervallen hinter den zpdK-Datenströmen, zu vermeiden.

[0121] KB kann die aus Abschnitt 3.2 bekannten Tests (soweit anwendbar) durchführen. KB hat beispielsweise die Quality of Service (QoS) der Verbindung zwischen B nach A zu überprüfen. Dies setzt KB in die Lage zu überprüfen, ob A versucht Teile der Konversation von B zu unterdrücken und somit aus der Aufzeichnung und Signatur zu entfernen. Wenn ein vorher bestimmter Schwellwert an verlorenen Paketen von B nach A überschritten wird, so kann z.B. KB die Kommunikation als nicht vertrauenswürdig ansehen. Insbesondere sind sowohl durch KA als auch durch KB die Sicherheitspolitiken aus Abschnitt 2.4.1 anwendbar.

[0122] Während der Signierung sollte allen Kommunikationsparteien die Durchführung der Signatur signalisiert werden, zum Beispiel wie dies im dritten Absatz von Abschnitt 4.1 beschrieben wird. Des Weiteren sollte die Signatur auch während einer Kommunikation von den Partnern absichtlich gestartet und auch beendet werden können, zum Beispiel um von einer mündlichen Aushandlung von Vertragsbedingungen zum Abschluss des Vertrages überzugehen. Dies muss den Teilnehmern vorher signalisiert und je nach Anwendungsfall auch bestätigt werden. Auch diese Zustimmung sollte aufgezeichnet werden und bereits durch die Signatur abgedeckt sein.

[0123] Am Ende der Signatur steht die Datenstruktur, welche bei KB archiviert werden muss oder von KB an ein ausgelagertes Archiv übergeben wird. Alle Intervalle werden wie in Fig. 7 gezeigt kontinuierlich gespeichert. Zeitstempel können zusätzlich hilfreich sein, eine aufgezeichnete, signierte zpdK auf einen exakten Zeitpunkt zu datieren. Das Speicherformat ist analog zur Archivierungsmethode aus Abschnitt 3 gebildet und entspricht dem in Fig. 3 gezeigten. Im Unterschied zu Fig. 3 werden hier die eigentlichen Datenpakete separat gespeichert. Diese Ausführungsvariante ergibt sich hier daraus, dass As Signatur nur über die Intervallmetadaten angewendet wird und damit nur über die Hash-Werte der Paketdaten, aber nicht über die Paketdaten selbst. Dies erlaubt es B, im Wesentlichen einfach die von A empfangenen gesicherten Intervallmetadaten abzuspeichern.

[0124] Das Format ist ein einfaches blockbasiertes, kontinuierliches Format, welches mit einem Start-Block beginnt, in dem die SIP-URIs der Kommunikationspartner, Zeitpunkt des Kommunikationsbeginns und die verwendeten Codecs erfasst sind. Folgende Intervalle werden durch B archiviert, wie sie produziert werden, was den Speicherbedarf der Methode im temporären Arbeitsspeicher auf die Größe eines Intervalls begrenzt. Am Ende einer Kommunikation wird ein spezieller Abschlussblock gespeichert, der den Abbruchgrund sowie Zeitpunkt erfasst.

[0125] Jeder mit einem Intervall verbundene Block beinhaltet die zugehörigen Pakete dieses Intervalls und mindestens die folgenden Zusatzinformationen: Die Richtung/Kanal des Intervalls, der Zeitpunkt, die

Liste der absoluten Paketnummern des Intervalls und die Hash-Werte der zugehörigen Pakete. Diese Zusatzinformationen werden z.B. in einem PKCS#7 Container signiert durch KA gespeichert. Der erste PKCS#7 Container muss zusätzlich die komplette Zertifikatskette speichern, auf die sich das Signaturzertifikat von A bezieht. Dies muss für die folgenden Container nicht erfolgen.

5.2 Mehrseitige Signatur

[0126] Wie in Abschnitt 5 bereits dargestellt kann die beschriebene Technik auch von beiden Seiten angewendet werden, um der jeweils anderen Seite ein von ihr signiertes Gespräch anzubieten, das dort dann archiviert werden kann. In diesem Fall gibt es keinen Partner, der den Signiervorgang zentral steuern würde. Es kann sogar passieren, dass die alternierende Verschränkung anders anfängt.

[0127] Eine bessere Lösung ist jedoch das Übersignieren durch beide Parteien, so dass jedes Intervall (also beispielsweise jede Sekunde des Gesprächs) erst von der einen Partei signiert wird und diese Signatur dann erneut von der zweiten Partei signiert wird. Erst danach setzt sich die Verkettung zum nächsten Intervall wie in Fig. 7 zu sehen fort. Beide Parteien erhalten nach Gesprächsende identische Aufzeichnungen, die einfach und effizient verglichen werden können. Die genaue Ausführung der Übersignatur ist in vielen Varianten möglich, von denen zwei erfindungsgemäße Varianten, die besonders sinnvoll erscheinen, vorgestellt werden. Der Übersicht halber werden die Darstellungen der Verfahren auf zwei Teilnehmer beschränkt. Die Methoden sind aber prinzipiell auch auf Konferenzen mit mehreren Teilnehmern anwendbar.

5.2.1 Variante A für zweiseitige Signaturen

[0128] Die in Fig. 4 und Fig. 6 beschriebenen Protokolle sind dazu wie folgt zu erweitern: Hierbei ist es vorteilhaft, einen Partner (z.B. den Anrufer) als steuernde Partei zu definieren. Nachdem in Fig. 4 die steuernde Partei KA eine Intervallsignatur an KB gesendet hat wartet sie mit dem nächsten Paket, bis KB auf diese Intervallsignatur geantwortet hat oder ein Timeout aufgetreten ist: KB signiert die ankommende Intervallsignatur mit seinem Signaturschlüssel, hängt sein Zertifikat an und sendet sie zurück. Dabei kann auch zur Bandbreitenersparnis nur die Signatur gesendet werden. Für das nächste Intervall (egal welcher Richtung) wird nun nicht der Hash des letzten von KA signierten Intervalls verwendet, sondern der Hash dieses übersignierten Pakets.

[0129] Für die Gegenrichtung in Fig. 6 wird ebenfalls eine Übersignierung durch KB eingeführt: Statt einer expliziten Quittierung sendet KB das übersignierte Intervallpaket zurück, so dass KA es speichern kann. Wieder kann auf die erneute Übertragung des von KA gesendeten Intervallpakets verzichtet werden, indem nur die Signatur gesendet wird.

[0130] Das sich auf beiden Seiten ergebende Datenformat ist in Fig. 8 dargestellt.

5.2.1 Bevorzugte Variante B für zweiseitige Signaturen

[0131] Die folgende Variante zum verketteten Übersignieren eines Gesprächs zwischen zwei Parteien ist stärker an die zuvor gezeigten Sicherungsmethoden angelehnt als Variante A. Im Prinzip erweitert und verallgemeinert sie die in Fig. 4 und Fig. 6 gezeigten Methoden zur einseitigen Signatur. Nun besitzen A und B Signaturschlüssel und Zertifikate. Das Verfahren ist symmetrisch bezüglich der ausgetauschten signierten Daten.

[0132] Im Folgenden wird die Methode zum Bilden von zweiseitig signierten Intervallen und ihrer Verkettung gezeigt.

[0133] Die Methode ist in Fig. 9 für die Senderichtung von A nach B skizziert, die andere Richtung funktioniert exakt gleich. KA sendet zpdK-Pakete an KB und sammelt sie in einem Zwischenspeicher, KB sammelt die empfangenen Pakete. Zu einem bestimmten Zeitpunkt, etwa dem Ablauf einer festgelegten Intervalldauer, führt KB das folgende aus: KB bildet eine Sicherung der empfangenen Pakete, etwa durch Hash-Werte der einzelnen Pakete. Dazu fügt KB wie in den oben geschilderten Methoden weitere Metadaten (Zeit, Richtung, etc.). Zudem fügt KB ein Sicherungsdatum des letzten Intervalls, z.B. einen Hash-Wert, hinzu. Wie dieser gebildet werden kann, wird weiter unten beschrieben. Diesen gesamten Datensatz sichert KB nun z.B. durch seine elektronische Signatur. Das signierte Datenpaket sendet er dann an KA. Es ersetzt bei der vorliegenden Methode die einfache Rückmeldung der empfangenen Pakete durch KB, wie sie in Fig. 4 gezeigt wurde. KA kann dem empfangenen, gesicherten Paket weitere Metadaten hinzufügen. Diese Gesamtheit von Daten bildet nun die Intervalldaten dieses Intervalls. Danach sichert KA diese Intervalldaten etwa durch Übersignieren. (Gegebenenfalls kann es reichen, wenn KA die Signatur von B und die von KA hinzugefügten Metadaten übersigniert, da die Signatur von B schon die von KB gesandten Daten sichert. Dazu muss KA aber unter Umständen zuvor die Signatur von B geprüft haben.) KA sendet die gesicherten Intervalldaten an KB. Beide Parteien sollten diese doppelt signierten Intervalldaten zusammen mit den darin referenzierten zpdK-Paketen abspeichern oder geeignet archivieren.

[0134] Das Senden redundanter Daten kann gemäß den in Abschnitt 2.3 beschriebenen Varianten ver-

mieden werden. Von KA muss außerdem im letzten Schritt nur die Signatur über das Datenpaket gesendet werden, als so genannte abgehängte (detached) Signatur, zuzüglich evtl. von ihm hinzugefügter und signierter Metadaten.

[0135] Die Verkettung wird nun erreicht, indem Sicherungsdaten dieses Intervalls auf geeignete Weise gesichert werden. Zum Beispiel kann ein Hash-Wert über die äußere, von KA angebrachte Signatur gebildet werden, oder über beide Signaturen (von A und B), oder über die gesamten Intervalldaten inklusive aller Signaturen. Letzteres ist unter Umständen zu bevorzugen, da dann keine Verifikation der schon angebrachten Signaturen nötig ist. Beide Parteien müssen für die Fortsetzung der Verkettung über diesen Sicherungswert (in der Fig. 9 mit V(N) bezeichnet) verfügen.

[0136] Zwei aufeinander folgende Intervalle N–1 und N sichern die Intervalldaten des Intervalls N–1 durch eine Signaturkette der Form BABA, BAAB, ABAB, oder ABBA. Damit ist für die Intervalldaten N–1 eine zweiseitige Nichtabstreitbarkeit erreicht, die dem bekannten BAKO-Protokoll entspricht. Dass heißt, beide Parteien sind sicher, dass die jeweils andere die von beiden Parteien signierten Daten des Intervalls N–1 besitzt.

[0137] Die Bildung des jeweils nächsten Intervalls kann auf verschiedene Weise angestoßen werden. Zum Beispiel kann von vornherein vereinbart sein, dass KA und KB alternierend Intervalle bilden, was etwa durch Zeitsteuerung – nach jeder Sekunde ist der jeweils andere an der Reihe – realisiert werden kann. Die genaue technische Ausführung ist hier offen gelassen.

[0138] Während des signierten Gesprächs können beide Parteien die bereits oben genannten Tests kontinuierlich durchführen. Z.B. können alle Sicherungswerte stichprobenweise oder kontinuierlich überprüft werden. Auch sollte bei der oben gezeigten Richtung KA prüfen, ob die von KB angeblich empfangenen Pakete einen ausreichenden QoS bieten, um die Verständlichkeit von A zu gewährleisten.

[0139] In Analogie zum BAKO-Protokoll kann das End-Intervall vom letzten Empfänger noch ein drittes Mal übersigniert und zurückgesandt werden, um auch für dieses den gleichen Grad an zweiseitiger Nichtabstreitbarkeit zu erreichen.

5.3 Erhöhung des Beweiswerts durch Verwendung vertrauenswürdiger Endgeräte

[0140] Um unter Verwendung der in Abschnitt 5 bisher dargestellten Methoden zu einer sicheren, vertrauenswürdigen Signaturerstellungseinheit für zpdK, z.B. gemäß des EU-Schriftstücks CEN CWA 14170 (European Committee for Standardization (CEN) Workshop Agreement CWA 14170: Security requirements for signature creation applications. Mai 2004. ftp://ftp.cenorm.be/PUBLIC/CWAs/eEurope/eSign/cwa14170-00-2004-May.pdf), zu gelangen, sind weitere technische Sicherungsmaßnahmen notwendig. Insbesondere müssen für Hard- und Software die geforderten Sicherheitseigenschaften nachweisbar sein.

[0141] Die im Weiteren beschriebene technische Realisierung von TA 5 fußt hierzu auf den von der Trusted Computing Group TCG erarbeiteten Standards für sichere Rechnerplattformen, so genannte Trusted Platforms (TP). Die Grundidee ist die Realisierung der zpdK-Signatureinheit als TP, wobei insbesondere die Verarbeitung und Übertragung von Sprachdaten durch TC-Methoden zu sichern ist.

[0142] Es ist hervorzuheben, dass die im Folgenden beschriebene technische Ausprägung über den Einsatzbereich von TA 5 hinaus relevant ist. TC kann ebenfalls in ähnlicher Weise in TA 2–4 eingeführt werden.

[0143] Mögliche technisch-kommerzielle Realisierungen des unten vorgestellten Konzeptes liegen besonders im Bereich der mobilen Kommunikation nahe. In der Tat deutet sich eine baldige Markteinführung von TC Technologie enthaltenden mobilen Endgeräten bereits an. Auch ist gerade die Mobilfunkindustrie in der TCG besonders aktiv. Gerade für elektronische Signaturen sind mobile Endgeräte, die sich wie üblicherweise Signatur-Token sowieso schon im Besitz des Unterzeichners befinden, attraktiv. Dies ermöglicht ggf. eine Vereinigung von Signatur-Token (klassisch das in einer Smartcard befindliche digitale Zertifikat und der geheime Schlüssel) und Signatur-Erstellungsgerät.

[0144] Fig. 10 zeigt das Schema eines TC-basierten, vertrauenswürdigen zpdK-Signiergeräts. Der Ablauf des Signierens ähnelt der gewöhnlichen elektronischen Signatur. Der Signierer weist sich dazu am Gerät durch Wissen und Besitz aus. Zur Erzeugung der eigentlichen elektronischen Signatur verwendet die Signaturerzeugungseinheit je nach Einsatzszenario im Gerät die Methode aus Abschnitt 5.1 oder 5.2. Hier wird weiterhin davon ausgegangen, dass Signaturen auf asymmetrischer Kryptografie beruhen und Identitäten durch digitale Zertifikate nachgewiesen werden (PKI). Die wesentliche Verwendung von TC besteht in folgenden Punkten, die auch die jeweilige technische Ausführung beschreiben.

1. Der TPM-basierte Trusted Boot Prozess überprüft beim Start des Gerätes die Unverändertheit seiner Komponenten gegenüber einem Referenzzustand. Das Ergebnis der Prüfungen wird aufgezeichnet und durch das TPM geschützt und kann später zum Nachweis der Unverändertheit der

Gerätefunktion gegenüber Dritten verwendet werden. Insbesondere misst der Trusted Boot Prozess die Integrität
a) der Signaturerzeugungssoftware, welche je nach Anwendungsszenario die Methode aus Abschnitt 5.1 oder 5.2 verwendet,
b) der Hard- und Softwarekomponenten die Audiodaten verarbeiten und weitergeben,
c) Der Ein- und Ausgabeeinheiten zur Signalisierung des Benutzers (Signierers) und Eingabe der Signatur-Token,
d) ggf. einer im Gerät enthaltenen hard- und/oder softwarebasierten vertrauenswürdigen Zeitquelle zur Verwendung im Signierprozeß gemäß Abschnitt 5.1 oder 5.2
2. Im TC-Prozess der Remote Attestation kann das Gerät von A nun gegenüber den Kommunikationspartnern die Unveränderthеit der im Trusted Boot Prozess gemessenen Komponenten nachweisen. Insbesondere weist A dadurch nach, dass er im Besitz eines vertrauenswürdigen Signaturterminals mit einem geschützten Audiokanal und geschützter Signaturerzeugungssoftware ist.
3. Der Audiokanal, d.h. die Soft- und Hardware im Gerät, die Audiodaten verarbeiten und weiterreichen, sind besonders geschützt, z.B. durch TC-Methoden der Verschlüsselung von Transportwegen und Nachweis der Integrität im Trusted Boot. Die besondere Bedeutung dieses Schutzes liegt darin, dass die zu signierenden Daten ausschließlich durch diesen I/O-Kanal laufen. Vorteilhaft ist hierbei insbesondere, dass nur der Audiokanal als einziger I/O-Kanal gesichert werden muss, wodurch die bei einem Signierterminal gewöhnlich nötige Sicherung von Tastatur und Bildschirm nicht nötig ist.
4. Eine TP-basierte zpdK-Signatureinheit kann insbesondere über eine vertrauenswürdige Zeitquelle, basierend auf einer zuverlässigen internen Uhr, oder aber auf einem zum Beispiel vom mobilen Netzbetreiber gelieferten Zeitnormal enthalten. Diese Zeitquelle kann wesentlich zur zeitlichen Festlegung des signierten Gesprächs gemäß Abschnitten 2.4.3, 4.1 und 5.1 verwendet werden.
5. Im Remote Attestation Prozess wird eine Zertifizierungsinstanz (Privacy CA, PCA) verwendet, die im Prinzip die Identität des von A verwendeten Gerätes bestätigen kann. Es ist möglich, diese Zertifizierungsinstanz zu verwenden, um die für die Signatur nötige Authentisierung zu erreichen. Das heißt, dass dann von der TP verwaltete so genannte Attestation Identity Keys (AIK) als zpdK-Signaturschlüssel verwendet werden. Sie sind mit einem Zertifikat der PCA versehen und weisen so die Identiät des Gerätes nach. Zusammen mit der üblichen Nutzerauthentisierung am Gerät, etwa mittels SIM-Karte und Eingabe der PIN oder direkt gegenüber des TPM, entstehen zusammengenommen die notwendigen Eigenschaften eines Signier-Tokens.
6. Wird im Unterschied zum vorherigen Punkt 5. eine externe PKI zur Zertifizierung der zpdK-Signaturschlüssel verwendet, so kann weiters TC benutzt werden, um die Sicherheit des Speichers, in dem Schlüssel und Zertifikate im Gerät aufbewahrt werden, herzustellen.

Patentansprüche

1. Verfahren zur Sicherung einer zeitkritischen, ein-, zwei- oder mehrseitigen und zumindest während eines Teilabschnitts der Übertragungsstrecke digitalen, paketbasierten Kommunikation zwischen mind. zwei Personen und/oder Maschinen, **dadurch gekennzeichnet**, dass die Integrität und/oder Nichtabstreitbarkeit für die Inhalte und/oder den Zeitpunkt und/oder den Ort und/oder die Identität der Gesprächspartner der Kommunikation durch eine während bestimmter Teile oder der gesamten Dauer der Kommunikation paketbasierten Anwendung digitaler technischer Sicherungsmethoden gewährleistet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die zu sichernde Kommunikation ein Telefongespräch, insbesondere Voice over IP (VoIP), eine Telefon- oder Videokonferenz oder ein textbasiertes Chat umfasst und die Kommunikation zumindest über einen Teilabschnitt der Übertragungsstrecke anhand des SIP/RTP-Protokolls, des Inter-Asterisk-Protokolls (AIX) oder des H.323-Protokolls durchgeführt wird.

3. Verfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass jeweils mehrere zu übertragende Pakete zu einem Intervall zusammengefasst werden, wobei bevorzugt ein Intervall nur Pakete einer Kommunikationsrichtung enthält, und jeweils für ein Intervall Intervalldaten I_N, bestehend aus den Paketen des Intervalls und Metadaten des Intervalls, gebildet werden; und auf jedes Intervall und die zugehörigen Intervalldaten eine oder mehrere technische Sicherungsmethoden K() angewendet werden und dabei ein oder mehrere Sicherungswerte gebildet werden.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass die Anzahl der Pakete pro Intervall der Sprachdauer einer Sekunde oder einer, zum Beispiel in Abhängigkeit der Speicher- und Rechenkapazität oder der Kanalqualität, dynamisch festgelegten Anzahl von Paketen entsprechen.

5. Verfahren nach einem der Ansprüche 3 oder 4, dadurch gekennzeichnet, dass die Metadaten des Intervalls vorzugsweise Datum und Uhrzeit des Intervalls und/oder die Kommunikationsrichtung und/oder die Liste der Paket-Sequenznummern der Pakete des Intervalls umfassen.

6. Verfahren nach einem der Ansprüche 3 bis 5, dadurch gekennzeichnet, dass die technischen Sicherungsmethoden K() die Anwendung eines Hash-Algorithmus und/oder die Anwendung eines keyed-hash message authentication code (HMAC) und/oder die Anbringung einer elektronischen Signatur und/oder die Anbringung eines elektronischen Zeitstempels umfassen.

7. Verfahren nach einem der Ansprüche 3 bis 6, dadurch gekennzeichnet, dass zur Überprüfung der Sicherung der Kommunikation ein Vergleich der in den Intervalldaten enthaltenen Zeitinformation mit der lokalen Systemzeit und/oder mit den Zeitangaben und Sequenznummern der Pakete durchgeführt wird.

8. Verfahren nach einem der Ansprüche 3 bis 7, dadurch gekennzeichnet, dass die Intervalle miteinander verkettet werden, wobei auch Intervalle verschiedener Kommunikationsrichtungen miteinander verkettet werden können, beispielsweise durch abwechselnde Sicherung von Intervallen verschiedener Kommunikationsrichtungen und deren Verkettung in dieser abwechselnden Reihenfolge.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass zur Verkettung der Intervalle für jedes Intervall N der zu sichernden Kommunikation der gebildete Sicherungswert V_N in das darauf folgende Intervall N+1 eingebettet wird und die Sicherungswerte $V_N = K(I_N, V_{N-1})$ jeweils über die Intervalldaten I_N und dem Sicherungswert des vorhergehenden Intervalls V_{N-1} gebildet werden.

10. Verfahren nach einem der Ansprüche 8 oder 9, dadurch gekennzeichnet, dass zur Verkettung der Intervalle zunächst für eine Sicherung der Intervalldaten eine erste technische Sicherungsmethode S(), beispielsweise eine elektronische Signatur, über die Intervalldaten und den Sicherungswert des vorhergehenden Intervalls V_{N-1} durchgeführt wird und dann entweder über $S(I_N, V_{N-1})$ oder über $S(I_N, V_{N-1})$ und den Intervalldaten I_N und/oder den Sicherungswert des vorhergehenden Intervalls V_{N-1} nochmals eine weitere technische Sicherungsmethode, beispielsweise ein Hash-Algorithmus, angewandt und dieser Sicherungswert V_N in das nächste Intervall eingebettet wird.

11. Verfahren nach einem der Ansprüche 8 bis 10, dadurch gekennzeichnet, dass eine Überprüfung der gesicherten Kommunikationsdaten durch Vergleich der in den Intervallen eingebetteten Sicherungswerte V_N mit den neu gebildeten Sicherungswerten der vorliegenden Intervalldaten durchgeführt wird.

12. Verfahren nach einem der Ansprüche 8 bis 11, dadurch gekennzeichnet, dass am Anfang und am Ende der Verkettung jeweils ein Anfangs- bzw. Endintervall zur Intervallverkettung verwendet wird, das aus Metadaten zur eindeutigen Identifizierung der zu sichernden Kommunikation besteht.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass die Metadaten im Anfangsintervall eine eindeutige Kennung der Kommunikationsteilnehmer und/oder Datum und Uhrzeit des Kommunikationsbeginns und/oder eine den fehlenden Sicherungswert des vorhergehenden Intervalls V_0 ersetzende Zufallszahl und/oder Informationen über die Art des übertragenen Medienformats und Codecs umfassen.

14. Verfahren nach einem der Ansprüche 12 oder 13, dadurch gekennzeichnet, dass die Metadaten im Endintervall den Sicherungswert des vorletzten Intervalls und/oder einen Flag, das anzeigt, dass dies das letzte Intervall der Kommunikation ist, und/oder den Grund für das Ende der Kommunikation umfassen.

15. Verfahren nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, dass zur Sicherung des Zeitpunktes der Kommunikation in Anfangs- und/oder Endintervall ein elektronischer Zeitstempel entweder in die Intervalldaten eingefügt und mitgesichert wird oder selbst zur nochmaligen Sicherung bereits gesicherter Intervalldaten dient.

16. Verfahren nach Anspruch 15, dadurch gekennzeichnet, dass zur Überprüfung des Zeitpunktes der Kommunikation die lokale Systemzeit oder der bewiesene Zeitpunkt der Kommunikation einer dritten Partei mit dem gesicherten elektronischen Zeitstempel verglichen wird.

17. Verfahren nach einem der Ansprüche 1 bis 16, dadurch gekennzeichnet, dass die Kanalqualität überprüft wird, beispielsweise durch Überwachung der Häufigkeit der Paketverluste anhand der Sequenznummern der Pakete, und bei Auftreten eines Unterlaufs, d.h. Absinken der Kanalqualität unter einen vorher zu bestimmenden Grenzwert, eine der folgenden Maßnahmen ergriffen wird:
a) der Unterlauf wird ignoriert; oder
b) Der Unterlauf wird dem/den Kommunikationspartner/n signalisiert und das Sicherungsverfahren wird fortgesetzt; oder
c) die Sicherung wird abgebrochen und die Kommunikation wird ungesichert weitergeführt; oder
d) die Kommunikation wird beendet.

18. Verfahren nach einem der Ansprüche 1 bis 17, dadurch gekennzeichnet, dass zur gesicherten Archivierung der Kommunikation an einem bestimmten Punkt der digitalen, paketbasierten Übertragungsstrecke, zum Beispiel auf Seiten der Kommunikationsendgeräte oder innerhalb der Kommunikationsvermittlungsgeräte, eine Sicherungskomponente

(VSec), welche die gesamte Kommunikation mithören kann, und eine Archivierungskomponente (Arc), in der die durch Vsec erzeugten Daten archiviert werden, eingefügt werden.

19. Verfahren nach Anspruch 18, dadurch gekennzeichnet, dass sich Vsec anhand der verwendeten technischen Sicherungsmethoden gegenüber Arc authentifizieren muss.

20. Verfahren nach einem der Ansprüche 18 oder 19, dadurch gekennzeichnet, dass als Kommunikationsgeräte Standardgeräte ohne Sicherungsfunktionen verwendet werden und VSec kontinuierlich während des Gesprächs die technischen Sicherungsmethoden auf die Kommunikationspakete anwendet, die Kanalqualität überwacht, und die gesicherten Daten an Arc übermittelt; und Arc Sicherheitsüberprüfungen durchführt und die gesicherten Daten speichert.

21. Verfahren nach einem der Ansprüche 3 bis 19, dadurch gekennzeichnet, dass in einer oder mehreren der die Sicherheitsmethoden durchführenden Komponenten, beispielsweise den beteiligten Kommunikationsgeräten, die Information, welche Pakete auf der Transportebene tatsächlich empfangen wurden, vorliegt, zum Beispiel durch Rückmeldung dieser Information an den Sender durch den Empfänger.

22. Verfahren nach Anspruch 21, dadurch gekennzeichnet, dass zur Behandlung von Paketverlusten auf der Transportebene die Intervalle nur mit den jeweils empfangenen Paketen gebildet und nur über diese Intervalldaten die technischen Sicherungsmethoden angewendet werden.

23. Verfahren nach Anspruch 21, dadurch gekennzeichnet, dass zur Behandlung von Paketverlusten auf der Transportebene über die einzelnen Pakete eine technische Sicherungsmethode, bevorzugt eine Hash-Funktion, angewendet wird und hierdurch Paketsicherungswerte gebildet werden.

24. Verfahren nach Anspruch 23, dadurch gekennzeichnet, dass die Paketsicherungswerte in die Intervalldaten eingefügt und der oder die Sicherungsmethoden zur Sicherung der Intervalldaten auf die gesamten Paketsicherungswerte und gegebenenfalls auf weitere Metadaten angewendet werden und der resultierende Sicherungswert zur Verkettung der Intervalle verwendet wird.

25. Verfahren nach Anspruch 23, dadurch gekennzeichnet, dass nur für die empfangenen Pakete Paketsicherungswerte erzeugt und in die Intervalldaten eingefügt werden und der oder die Sicherungsmethoden zur Sicherung der Intervalldaten auf diese Paketsicherungswerte und gegebenenfalls weitere Metadaten angewendet werden und der resultierende Sicherungswert zur Verkettung der Intervalle verwendet wird.

26. Verfahren nach Anspruch 25, dadurch gekennzeichnet, dass die erzeugten Paketsicherungswerte zur Sicherung des Intervalls verwendet aber nicht in die Intervalldaten eingefügt werden.

27. Verfahren nach den Ansprüchen 1 bis 19 oder 21 bis 26, dadurch gekennzeichnet, dass die Sicherungsverfahren von den Kommunikationsteilnehmern während der Kommunikation gestartet und beendet werden können; und dies den Kommunikationsteilnehmern signalisiert wird und die Kommunikationsteilnehmer gegebenenfalls hierzu Ihre Zustimmung geben.

28. Verfahren nach einem der Ansprüche 21 bis 27, dadurch gekennzeichnet, dass für die Sicherung der Authentizität eines Kommunikationspartners A gegenüber einem Kommunikationspartner B zu Beginn der Kommunikation eine Authentisierung von A durchgeführt und die zugehörigen Informationen in das Startintervall eingefügt werden; und lediglich eine Sicherung der Kommunikationsdaten in der Kommunikationsrichtung von A nach B notwendig ist und die gebildeten Intervallsicherungswerte von dem Kommunikationsgerät von A (KA) an das Kommunikationsgerät von B (KB) gesendet werden und KB damit kontinuierlich die Authentizität von A überprüfen kann.

29. Verfahren nach Anspruch 28, dadurch gekennzeichnet, dass die laufende Durchführung der Authentizitätsprüfung den Kommunikationspartnern signalisiert wird.

30. Verfahren nach einem der Ansprüche 21 bis 27, dadurch gekennzeichnet, dass für die einseitige Willenserklärung eines Kommunikationspartners A gegenüber einem Kommunikationspartnerm B zur späteren Nichtabstreitbarkeit der Kommunikation von Seiten A eine Intervallsicherung beider Kommunikationsrichtungen bzgl. der Identität des Kommunikationspartners A, des Datums und der Uhrzeit und des Kommunikationsinhalts und deren Intervallverkettung durchgeführt wird; und die von KA gebildeten Intervallsicherungsdaten an KB gesendet werden; und KB kontinuierlich Sicherheitsüberprüfungen durchführt und die Kommunikation inklusive der Sicherungsdaten speichert.

31. Verfahren nach einem der Ansprüche 21 bis 27, dadurch gekennzeichnet, dass für die gegenseitige Willenserklärung eines Kommunikationspartners A gegenüber einem Kommunikationspartner B und umgekehrt zur späteren Nichtabstreitbarkeit der Kommunikation von Seiten A und von Seiten B jeweils eine Sicherung der einseitigen Willenserklärung von A gegenüber B und von B gegenüber A durchgeführt, überprüft und gespeichert wird.

32. Verfahren nach einem der Ansprüche 21 bis 27, dadurch gekennzeichnet, dass für die gegenseitige Willenserklärung eines Kommunikationspartners A gegenüber einem Kommunikationspartner B und umgekehrt zur späteren Nichtabstreitbarkeit der Kommunikation von Seiten A und von Seiten B die Intervalle zunächst durch eine elektronische Signatur eines Kommunikationspartners und danach durch das Übersignieren des anderen Kommunikationspartners gesichert werden, die Verkettung durch Sicherungswerte, die über von beiden Kommunikationspartnern signierte Intervallsicherungswerte und optional über die Intervalldaten gebildet werden, durchgeführt wird und die gesamte Kommunikation inklusive der Sicherungsdaten von KA und/oder KB kontinuierlich überprüft und gespeichert wird.

33. Verfahren nach Anspruch 32, dadurch gekennzeichnet, dass anstatt der Rückmeldung, welche Pakete eines Intervalls empfangen wurden bereits Intervallsicherungswerte zum Zwecke des Übersignierens durch den Kommunikationspartner zurückgesendet und/oder anstatt der Bestätigung des Empfangs von Intervallsicherungsdaten übersignierte Intervallsicherungsdaten zurückgesendet werden.

34. Verfahren nach einem der Ansprüche 28 bis 33, dadurch gekennzeichnet, dass die Sendung der Intervallsicherungsdaten zwischen zwei Kommunikationsgeräten mit geeigneten Transportprotokollen gegen Datenverluste gesichert wird.

35. Verfahren nach einem der Ansprüche 28 bis 34, dadurch gekennzeichnet, dass die Verkettung von Intervallen verschiedener Kommunikationsrichtungen in dynamischer Reihenfolge erfolgt, z.B. je nach dem für welche Kommunikationsrichtung genügend Pakete für eine Intervallbildung gerade empfangen bzw. als empfangen rückbestätigt wurden.

36. Vorrichtung zur Sicherung einer zeitkritischen, ein-, zwei- oder mehrseitigen und zumindest während eines Teilabschnitts der Übertragungsstrecke digitalen, paketbasierten Kommunikation zwischen mind. zwei Personen und/oder Maschinen, mit einer oder mehrerer Einrichtungen zur Gewährleistung der Integrität und/oder Nichtabstreitbarkeit für die Inhalte und/oder den Zeitpunkt und/oder den Ort und/oder die Identität der Gesprächspartner der Kommunikation durch während bestimmter Teile oder der gesamten Dauer der Kommunikation paketbasierte Anwendung digitaler technischer Sicherungsmethoden.

Es folgen 10 Blatt Zeichnungen

Anhängende Zeichnungen

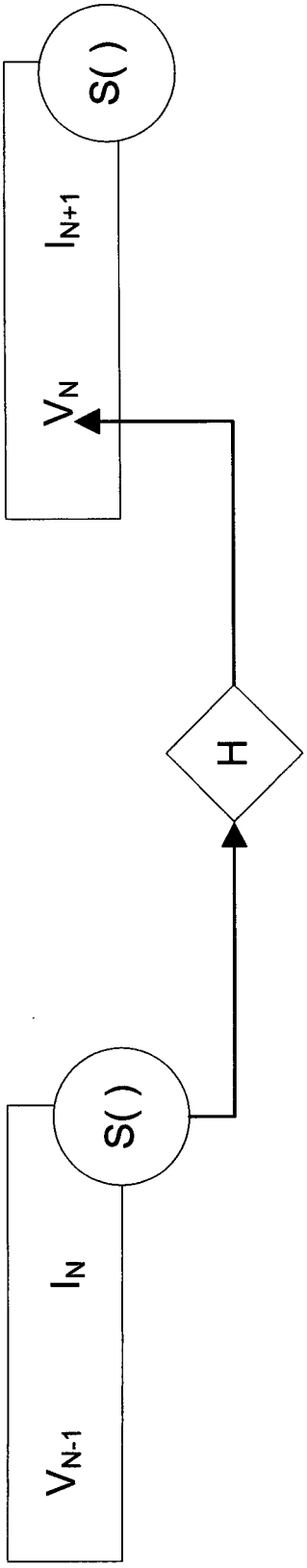


Fig. 1

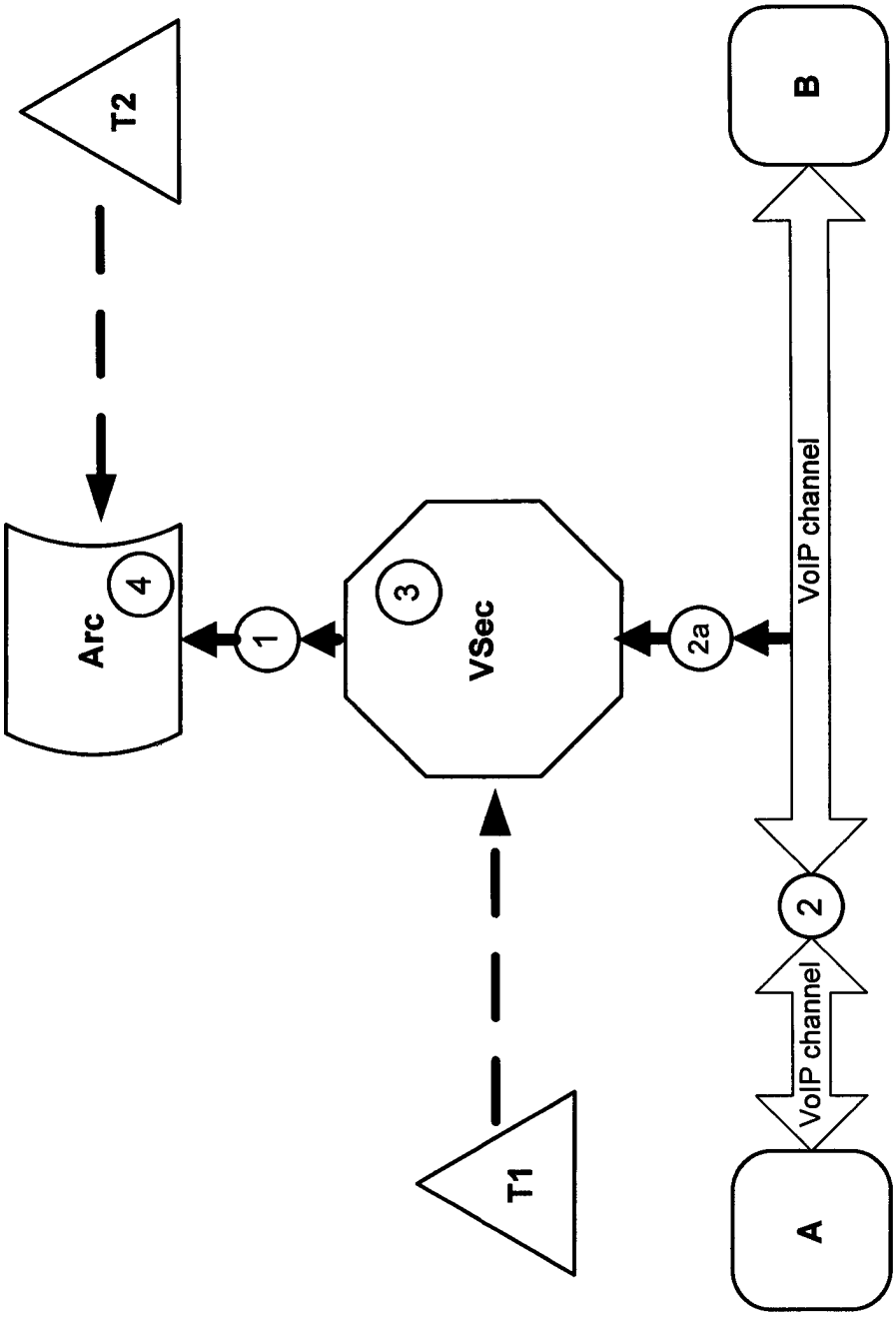


Fig. 2

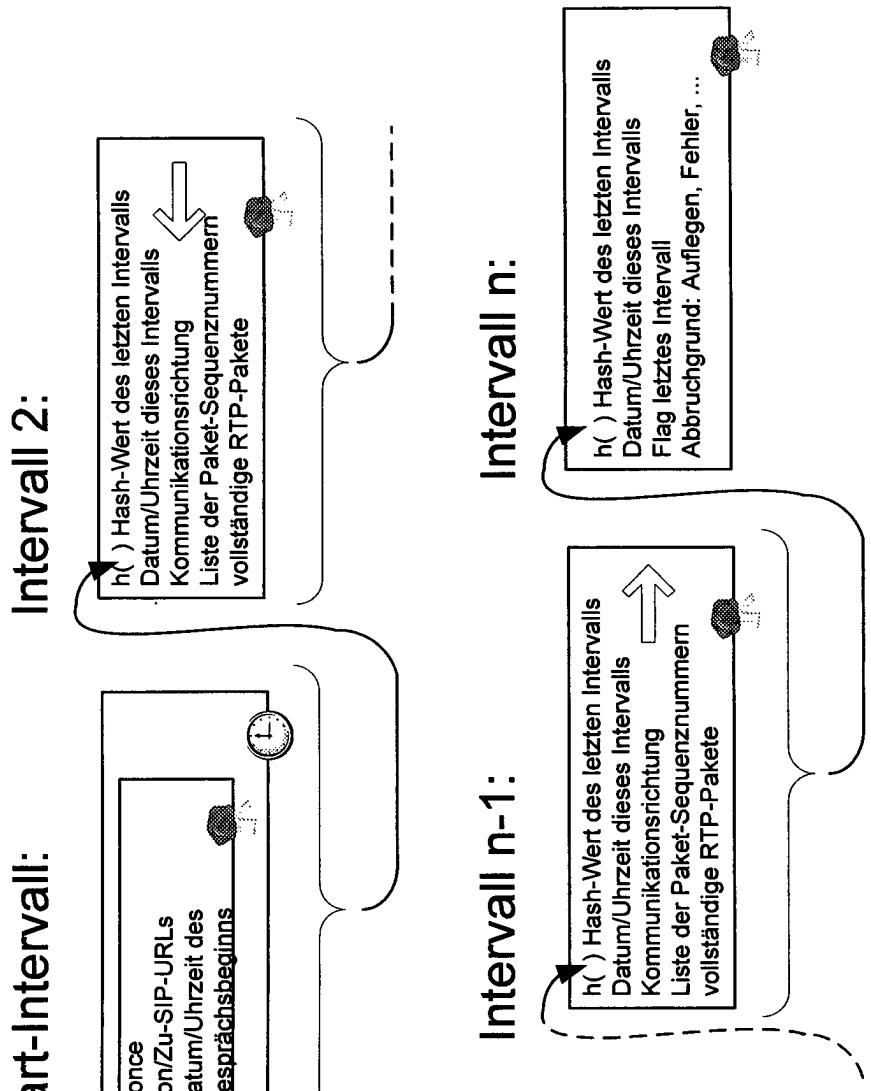

Start-Intervall:
Nonce
Von/Zu-SIP-URLs
Datum/Uhrzeit des
Gesprächsbeginns
Intervall 2:
h( ) Hash-Wert des letzten Intervalls
Datum/Uhrzeit dieses Intervalls
Kommunikationsrichtung
Liste der Paket-Sequenznummern
vollständige RTP-Pakete
Intervall n-1:
h( ) Hash-Wert des letzten Intervalls
Datum/Uhrzeit dieses Intervalls
Kommunikationsrichtung
Liste der Paket-Sequenznummern
vollständige RTP-Pakete
Intervall n:
h( ) Hash-Wert des letzten Intervalls
Datum/Uhrzeit dieses Intervalls
Flag letztes Intervall
Abbruchgrund: Auflegen, Fehler, ...

Fig. 3

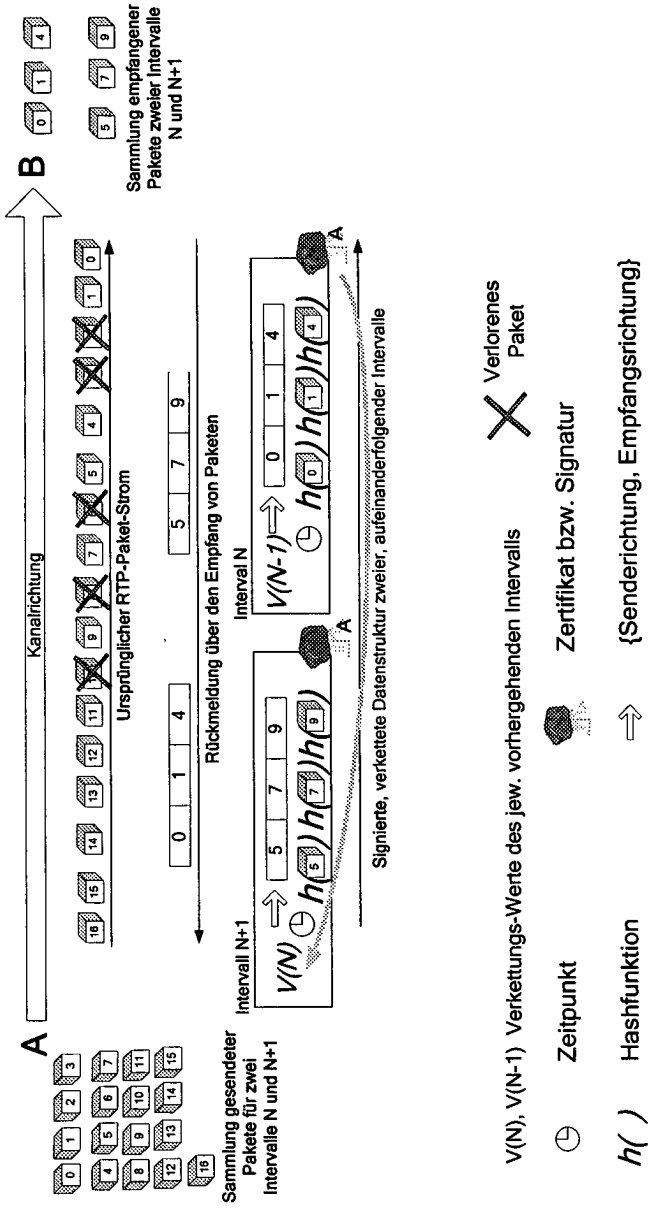

A
B
Kanalrichtung
Ursprünglicher RTP-Paket-Strom
Sammlung gesendeter Pakete für zwei Intervalle N und N+1
Sammlung empfangener Pakete zweier Intervalle N und N+1
Rückmeldung über den Empfang von Paketen
Intervall N+1
Interval N
V(N)
V(N-1)
Signierte, verkettete Datenstruktur zweier, aufeinanderfolgender Intervalle
V(N), V(N-1) Verkettungs-Werte des jew. vorhergehenden Intervalls
Verlorenes Paket
Zeitpunkt
Zertifikat bzw. Signatur
h( ) Hashfunktion
{Senderichtung, Empfangsrichtung}

Fig. 4

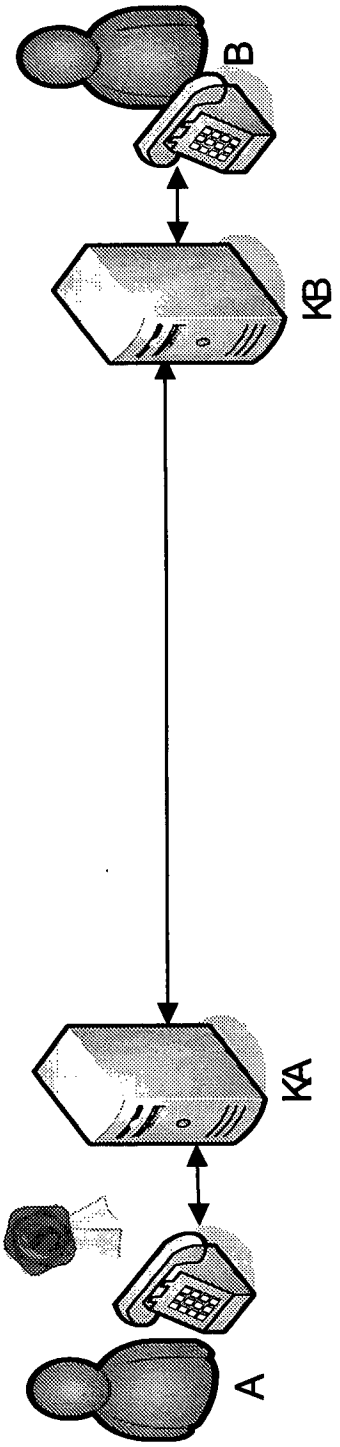


Fig. 5

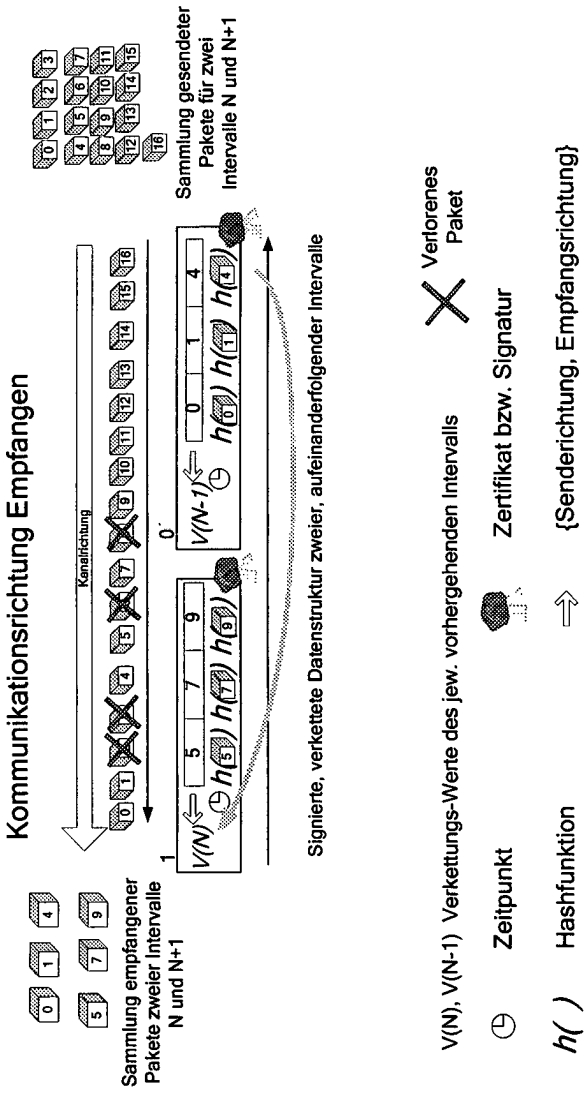

Kommunikationsrichtung Empfangen
Kanalrichtung
Sammlung empfangener Pakete zweier Intervalle N und N+1
Sammlung gesendeter Pakete für zwei Intervalle N und N+1
Signierte, verkettete Datenstruktur zweier, aufeinanderfolgender Intervalle
V(N), V(N-1) Verkettungs-Werte des jew. vorhergehenden Intervalls
Verlorenes Paket
Zeitpunkt
Zertifikat bzw. Signatur
h( ) Hashfunktion
{Senderichtung, Empfangsrichtung}

Fig. 6

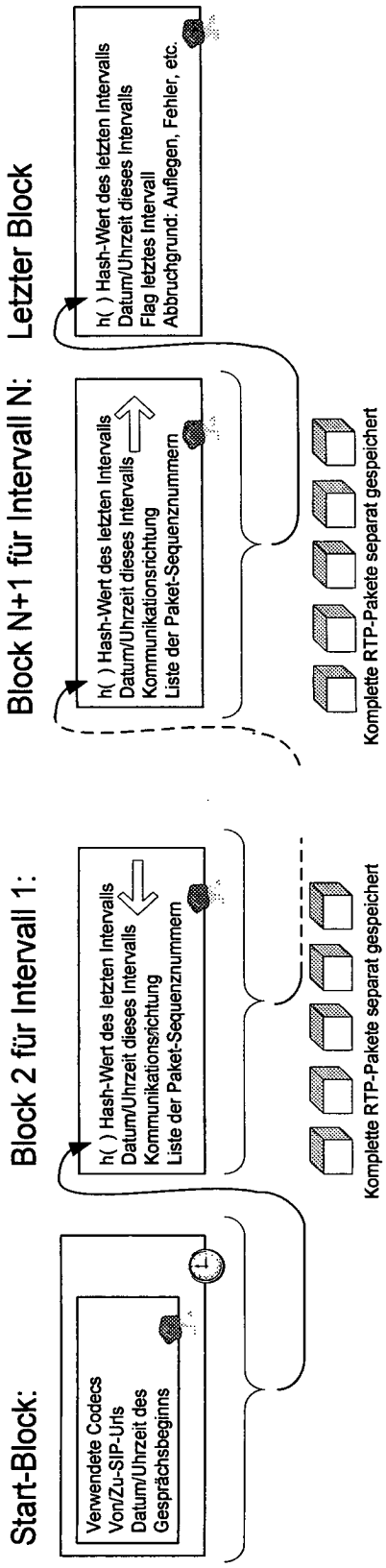

Start-Block:
Verwendete Codecs
Von/Zu-SIP-Urls
Datum/Uhrzeit des
Gesprächsbeginns
Block 2 für Intervall 1:
h( ) Hash-Wert des letzten Intervalls
Datum/Uhrzeit dieses Intervalls
Kommunikationsrichtung
Liste der Paket-Sequenznummern
Komplette RTP-Pakete separat gespeichert
Block N+1 für Intervall N:
h( ) Hash-Wert des letzten Intervalls
Datum/Uhrzeit dieses Intervalls
Kommunikationsrichtung
Liste der Paket-Sequenznummern
Komplette RTP-Pakete separat gespeichert
Letzter Block
h( ) Hash-Wert des letzten Intervalls
Datum/Uhrzeit dieses Intervalls
Flag letztes Intervall
Abbruchgrund: Auflegen, Fehler, etc.

Fig. 7

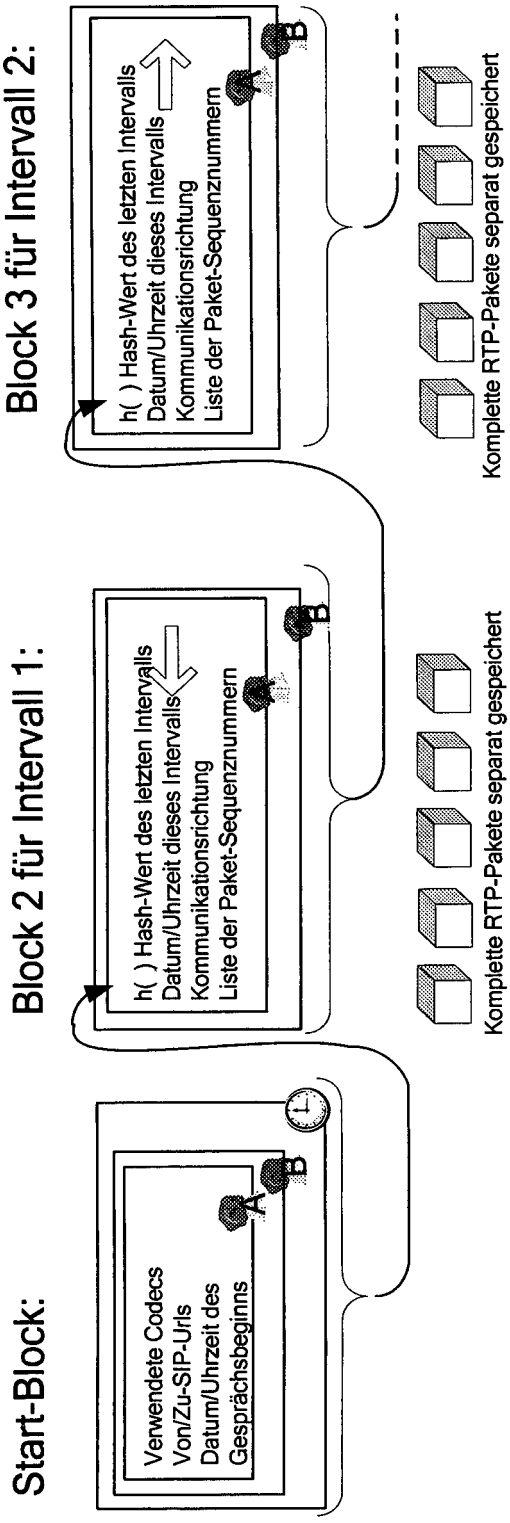

Start-Block:
Verwendete Codecs
Von/Zu-SIP-Urls
Datum/Uhrzeit des
Gesprächsbeginns
A
B
Block 2 für Intervall 1:
h( ) Hash-Wert des letzten Intervalls
Datum/Uhrzeit dieses Intervalls
Kommunikationsrichtung
Liste der Paket-Sequenznummern
A
B
Komplette RTP-Pakete separat gespeichert
Block 3 für Intervall 2:
h( ) Hash-Wert des letzten Intervalls
Datum/Uhrzeit dieses Intervalls
Kommunikationsrichtung
Liste der Paket-Sequenznummern
A
B
Komplette RTP-Pakete separat gespeichert

Fig. 8

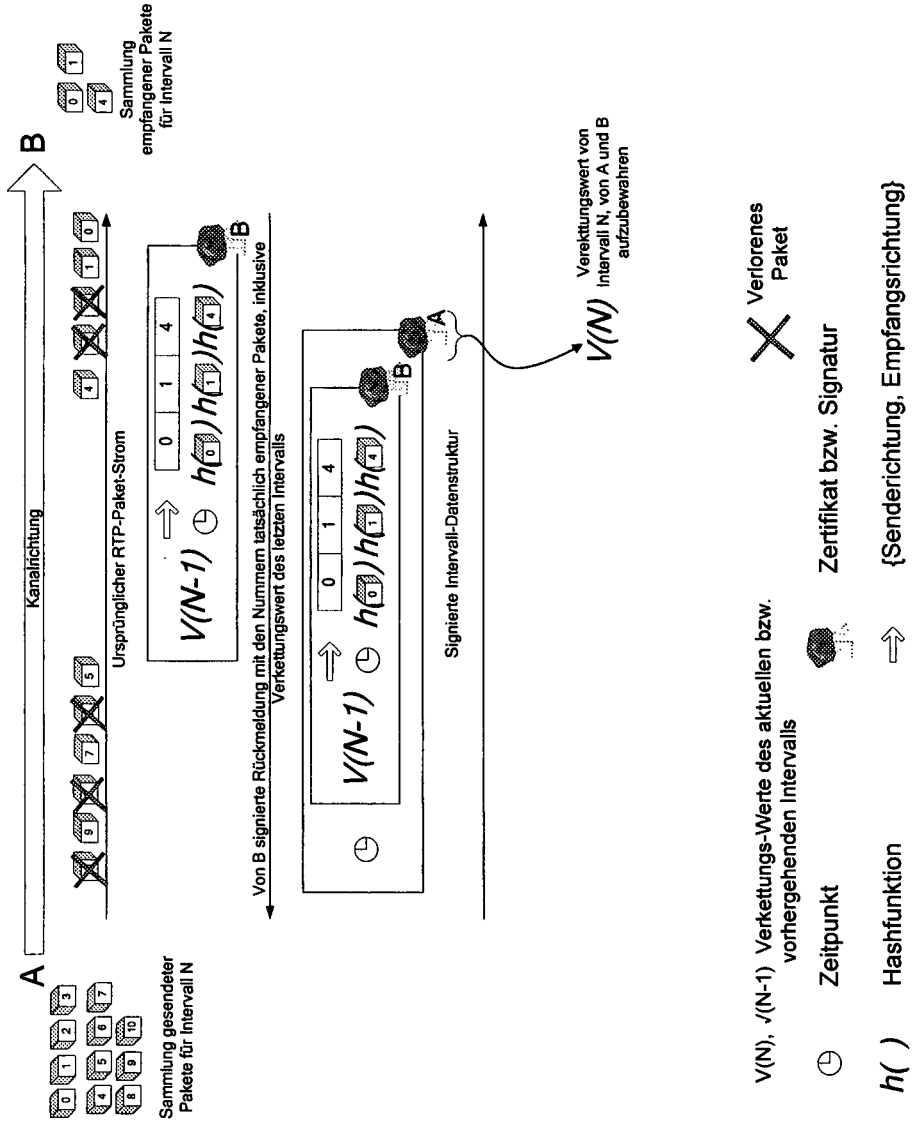

A
B
Kanalrichtung
Sammlung gesendeter Pakete für Intervall N
Ursprünglicher RTP-Paket-Strom
Sammlung empfangener Pakete für Intervall N
Von B signierte Rückmeldung mit den Nummern tatsächlich empfangener Pakete, inklusive Verkettungswert des letzten Intervalls
V(N-1)
h( ) h( ) h( )
Signierte Intervall-Datenstruktur
Verkettungswert von Intervall N, von A und B aufzubewahren
V(N)
Verlorenes Paket
V(N), V(N-1) Verkettungs-Werte des aktuellen bzw. vorhergehenden Intervalls
Zeitpunkt
Zertifikat bzw. Signatur
h( ) Hashfunktion
{Senderichtung, Empfangsrichtung}

Fig. 9

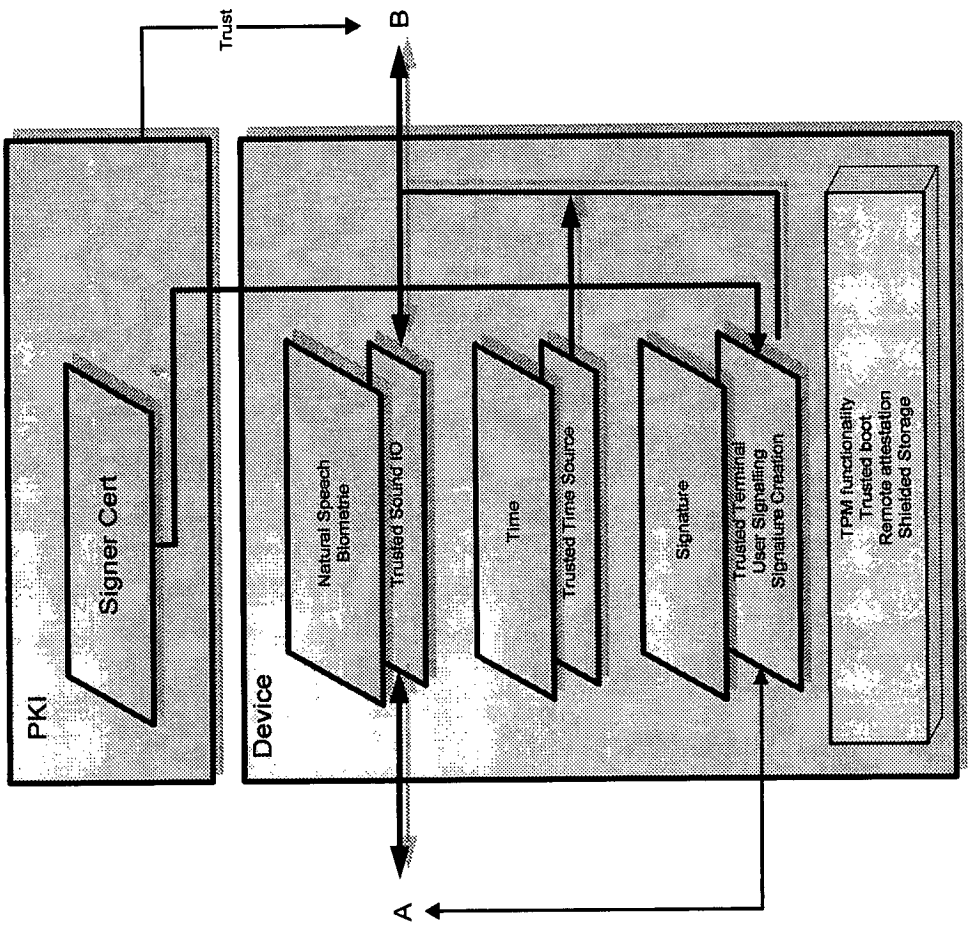

Trust
B
PKI
Signer Cert
Device
Natural Speech Biometrie
Trusted Sound ID
Time
Trusted Time Source
Signature
Trusted Terminal User Signaling Signature Creation
TPM functionality
Trusted boot
Remote attestation
Shielded Storage
A

Fig. 10