(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
10. Februar 2005 (10.02.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/013551 A1

(51) Internationale Patentklassifikation[7]: H04L 9/32, 12/58, 29/06

(21) Internationales Aktenzeichen: PCT/EP2004/007728

(22) Internationales Anmeldedatum:
13. Juli 2004 (13.07.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 33 048.8 18. Juli 2003 (18.07.2003) DE

(71) Anmelder und
(72) Erfinder: **KRAUSE, Georg** [DE/SG]; Block 23, Simei Street 4, #11-03, Singapore 529880 (SG).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **HARTONO, Rudy** [ID/SG]; 418 Choa Chu Kang, Avenue 4, #04-298, Singapore (SG).

(74) Anwalt: **KAMPFENKEL, Klaus**; Blumbach, Kramer & Partner GbR, Alexandrastrasse 5, 65187 Wiesbaden (DE).

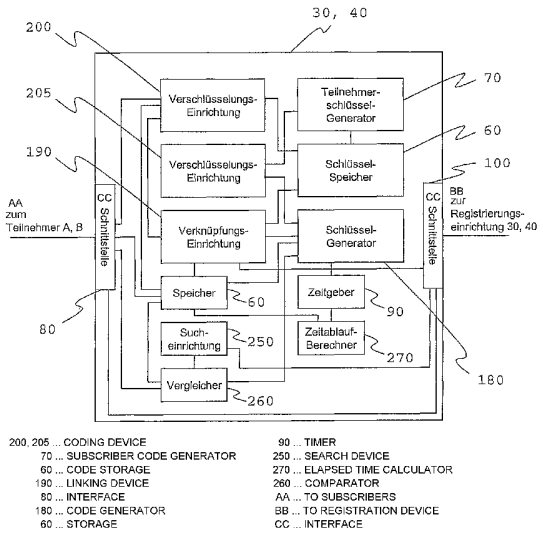
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND SECURITY SYSTEM FOR RECOGNIZING AN UNALTERED SUBSCRIBER IDENTITY IN A RECEIVER

(54) Bezeichnung: VERFAHREN UND SICHERHEITSSYSTEM ZUM ERKENNEN EINER UNVERFÄLSCHTEN TEILNEHMER-IDENTITÄT BEI EINEM EMPFÄNGER



(57) Abstract: The invention relates to a method and a security system for recognizing the unaltered identity of a subscriber who sends a message in a subscriber receiving said message, wherein the subscribers can be interconnected by means of a computer network, particularly the public Internet. The invention also relates to a registering device to be used in the security system. The invention also aims at solving the technical problem of providing the receiver with an improved mechanism for blocking web information (spam) sent via email. This is achieved in that the subscribers (10, 20) are registered in the registering devices (30, 40) and in that a method is provided, which makes it possible for the receiver of a message to verify the integrity of the identity of the sender of the information..

[Fortsetzung auf der nächsten Seite]

WO 2005/013551 A1

ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Veröffentlicht:

— *mit internationalem Recherchenbericht*

(57) Zusammenfassung: Die Erfindung betrifft ein Verfarhen sowie ein Sicherheitssystem zum Erkennen einer unverfälschten Identität eines eine Nachricht sendenden Teilnehmers bei einem diese Nachricht empfangenden Teilnehmer, wobei die Teilnehmer über ein Computernetz, insbesondere das öffentliche Internet, miteinander verbunden werden können. Ferner ist die Erfindung auf eine Registrierungseinrichtung zum Einsatz in dem Sicherheitssystem gerichtet. Der Erfindung liegt unter anderem das Technische Problem zugrunde, dem Empfänger von per E-mail versandter Werbeinformationen (Spam) einen verbesserten Mechanismus zum Sperren solcher Informationen bereitzustellen. Die wird dadurch erreicht, dass sich die Teilnehmer (10, 20) in Registrierungseinrichtung (30, 40) registrieren lassen und dass ein Verfahren bereitgestellt wird, welches dem Empfänger einer Nachricht ermöglicht, die Identität des Senders der Information auf Unversehrtheit hin zu prüfen.

Verfahren und Sicherheitssystem zum Erkennen einer unverfälschten Teilnehmer-Identität bei einem Empfänger

Beschreibung

Die Erfindung betrifft ein Verfahren sowie ein Sicherheitssystem zum Erkennen einer unverfälschten Identität eines eine Nachricht sendenden Teilnehmers bei einem diese Nachricht empfangenden Teilnehmer, wobei die Teilnehmer über ein Computernetz, insbesondere das öffentliche Internet, miteinander verbunden werden können. Ferner ist die Erfindung auf eine Registrierungseinrichtung zum Einsatz in dem Sicherheitssystem gerichtet.

Ein Nachteil bei bestehenden Computernetzen, wie zum Beispiel dem öffentlichen Internet ist, dass Absenderinformationen häufig nicht angegeben oder gefälscht werden. So führt die regelmäßige Fälschung von Absenderadressen dazu, dass zum Beispiel unerwünschte e-mail Werbesendungen beim Empfänger nicht wirkungsvoll mit Filtertechniken unterdrückt werden können. Dies hat zur Folge, dass der Anteil an ungewünschten Informationen rasch ansteigt und somit Speicherkapazität belegt wird. In bestehenden Netzwerkprotokollen wie dem Internet Protokoll oder den bei e-mail genutzten Protokollen gibt es keine Mechanismen die eine gesicherte Überprüfung der Absendeidentität ermöglichen.

Derzeit sind zwar eine Reihe von Verfahren bekannt, die alle mit Hilfe digitaler Signaturen eine Identität des Absenders nachweisen. Die Verfahren gehen jedoch davon aus,

dass es im Interesse des Absenders liegt seine Identität einwandfrei nachzuweisen. Es ist bei den bekannten Verfahren somit eine kooperative Unterstützung des Absenders erforderlich.

Verfahren, die den Absender zwingen, seine Identität offenzulegen, sind derzeit nicht bekannt. Das bekannte Problem mit unerwünschter Werbepost im Internet (Spam) würde sonst nicht existieren.

Die Erfindung liegt somit die Aufgabe zugrunde, ein Verfahren, ein Sicherheitssystem sowie eine Registrierungseinrichtung zur Verfügung zu stellen, mit denen es möglich ist, beim Empfänger einer Nachricht zu erkennen, dass die Identität des Nachrichten-Absenders nicht verfälscht worden ist.

Das oben genannte technische Problem löst die Erfindung zum einen durch die Merkmale des Anspruchs 1.

Danach wird ein Verfahren zum Erkennen einer unverfälschten Identität eines eine Nachricht sendenden Teilnehmers bei einem diese Nachricht empfangenden Teilnehmer bereitgestellt. Die Teilnehmer können über ein Computernetz miteinander verbunden werden. Das Verfahren weist folgende Schritte auf:
Die individuellen Identitäten mehrerer Teilnehmer werden in wenigstens einer Registierungseinrichtung gespeichert;
für jeden Teilnehmer wird wenigstens ein individueller Teilnehmerschlüssel erzeugt;
vor Beginn der Übertragung einer Nachricht von einem Ursprungsteilnehmer zu wenigstens einem Zielteilnehmer wird geprüft, ob die individuellen Identitäten der Ursprungs- und Zielteilnehmer in der wenigstens einen Registrierungseinrichtung gespeichert sind;

wenn dem so ist, wird die Identität des Ursprungsteilnehmers mit dem individuellen Teilnehmerschlüssel des Zielteilnehmers verschlüsselt wird und ein erster verschlüsselter Wert gebildet;
der erste verschlüsselte Wert wird zum Ursprungsteilnehmer übertragen;
eine Nachricht, die Identität des Ursprungsteilnehmers und der erste verschlüsselte Wert werden vom Urprungsteilnehmer zum Zielteilnehmer gesendet;
der erste verschlüsselte Wert wird mit dem individuellen Teilnehmerschlüssel des Zielteilnehmers entschlüsselt, um die entschlüsselte Identität des Ursprungsteilnehmers zu erhalten;
die entschlüsselte Identität des Ursprungsteilnehmers wird mit unverschlüsselt übertragenen Identität des Ursprungsteilnehmers verglichen;
bei Übereinstimmung der verglichenen Identitäten wird die empfangene Nachricht zur Weiterverarbeitung weitergeleitet.

Auf diese Weise wird sichergestellt, dass vom Zielteilnehmer nur Nachrichten zur Weiterverarbeitung - z. B. zur Speicherung, Ausgabe über ein Display - zugelassen werden, die von einem Ursprungsteilnehmer mit unverfälschter Identität empfangen worden sind.

Um zu verhindern, dass die empfangene Nachricht auf dem Übertragungswege manipuliert werden kann, wird die Nachricht in geeigneter Weise gesichert, zum Beispiel verschlüsselt. Dies erreicht die Erfindung durch folgende Schritte:
Wenn der Vergleich ergibt, dass die vom Ursprungsteilnehmer gesendeten individuellen Identitäten, nämlich die Identität des Ursprungs- und Zielteilnehmers in der wenigstens einen Registrierungseinrichtung gespeichert sind, wird ein kryptografischer Schlüssel erzeugt;

der kryptografische Schlüssel wird mit der Identität des Ursprungsteilnehmers verknüpft, wobei der erhaltende Wert dann mit dem individuellen Teilnehmerschlüssel des Zielteilnehmers verschlüsselt wird und den ersten verschlüsselten Wert bildet;
der kryptografische Schlüssel wird mit dem individuellen Teilnehmerschlüssel des Ursprungsteilnehmers verschlüsselt und bildet einen zweiten verschlüsselten Wert;
der erste und zweite verschlüsselte Wert werden zum Ursprungsteilnehmer übertragen;
der Ursprungsteilnehmer entschlüsselt den zweiten verschlüsselten Wert mit dem individuellen Teilnehmerschlüssel des Ursprungsteilnehmers, um den kryptografischen Schlüssel zu gewinnen;
die zu versendende Nachricht wird unter Verwendung des kryptografischen Schlüssels gesichert, beispielsweise verschlüsselt;
die gesicherte Nachricht, die Identität des Ursprungsteilnehmers und der erste verschlüsselte Wert werden vom Urprungsteilnehmer zum Zielteilnehmer gesendet;
der erste verschlüsselte Wert wird mit dem individuellen Teilnehmerschlüssel des Zielteilnehmers entschlüsselt, um die entschlüsselte Identität des Ursprungsteilnehmers und den kryptografischen Schlüssel zu erhalten;
die entschlüsselte Identität des Ursprungsteilnehmers wird mit unverschlüsselt übertragenen Identität des Ursprungsteilnehmers verglichen;
bei Übereinstimmung der verglichenen Identitäten wird die empfangene Nachricht mit dem kryptografischen Schlüssel entsichert, beispielsweise entschlüsselt, und zur Weiterverarbeitung weitergeleitet.

Der Sicherheitsgrad des Verfahrens kann dadurch erhöht werden, dass die Nutzungsdauer des kryptografischen Schlüssels für den Ursprungsteilnehmer und/oder den

Zielteilnehmer zeitlich begrenzt wird.

Dazu wird der Zeitpunkt der Erzeugung des kryptografischen Schlüssel ermittelt und gespeichert. Die Nutzung des kryptografischen Schlüssels durch den Ursprungs- und/oder Zielteilnehmer wird nach Ablauf einer vorbestimmten Zeitspanne mit Bezug auf den ermittelten Zeitpunkt gesperrt.

Das Verfahren ist auch anwendbar, wenn Ursprungs- und Zielteilnehmer unterschiedlichen Registrierungseinrichtungen zugeordnet sind.

Dies wird dadurch erreicht, dass vor Beginn der Übertragung einer Nachricht der Ursprungsteilnehmer die individuellen Identitäten der Ursprungs- und Zielteilnehmer an die ihm zugeordnete Registrierungseinrichtung sendet;
es wird dann geprüft, ob die individuellen Identitäten des Ursprungs- und Zielteilnehmers in dieser Registrierungseinrichtung gespeichert sind;
wenn nur die individuelle Identität des Ursprungteilnehmers gespeichert ist, wird die Registrierungseinrichtung gesucht, in der die Identität des Zielteilnehmers gespeichert ist.

Mit Hilfe des Verfahrens ist es möglich, empfängerseitig die Teilnehmer festzulegen, deren gesendete Nachrichten gezielt verworfen oder akzeptiert werden sollen. Auf diese Weise kann per E-mail versandter Werbeabfall (Spam) gezielt abgefangen werden. Hierzu werden in den Teilnehmern vorbestimmte Identitäten anderer Teilnehmer gespeichert, deren gesendete Nachrichten bei einem entsprechenden Zielteilnehmer verworfen oder weitergeleitet werden. Vorzugsweise handelt es sich bei den Identitäten um Teilnehmeradressen, insbesondere E-mail-Adressen.

Der kryptografische Schlüssel kann nach einem herkömmlichen Zufallsalgorithmus erzeugt werden.

Das oben genannte technische Problem wird ebenfalls durch ein

Sicherheitssystem zur gesicherten Übertragung einer Teilnehmer-Identität von einem Ursprungsteilnehmer zu einem Zielteilnehmer gelöst. Das Sicherheitssystem umfasst ein Kommunikationsnetz, insbesondere ein öffentliches Computernetz, wenigstens zwei Teilnehmer, die als Ursprungs- und/oder Zielteilnehmer fungieren können und an das Kommunikationsnetz angeschlossen sind, sowie wenigstens eine den Teilnehmern zugeordnete Registrierungseinrichtung.

Die Registrierungseinrichtung weist folgende Merkmale auf:

wenigstens eine Teilnehmer-Anschlussschnittstelle,

eine Speichereinrichtung, in der wenigstens die Identität eines Teilnehmers gespeichert ist,

eine Einrichtung zum Erzeugen individueller Teilnehmerschlüssel unter Ansprechen auf die wenigstens eine gespeicherte Identität und zum Senden der individuellen Teilnehmerschlüssel zu den dazugehörenden Teilnehmern,

eine Einrichtung zum Vergleichen der von einem Ursprungs- und/oder Zielteilnehmer gesendeten Identität mit den gespeicherten Identitäten,

eine erste Einrichtung zum Verschlüsseln der Identität des Ursprungsteilnehmers mit dem individuellen Teilnehmerschlüssel des Zielteilnehmers, so dass ein erster verschlüsselter Wert entsteht, der für den Ursprungsteilnehmer bestimmt ist,

wobei der Ursprungsteilnehmer folgende Merkmale aufweist:

eine Einrichtung zur Kommunikation mit der Registrierungseinrichtung und dem Zielteilnehmer, wobei der Zielteilnehmer folgende Merkmale aufweist:

eine Einrichtung zum Entschlüsseln des ersten verschlüsselte Wert mit dem individuellen

Teilnehmerschlüssel des Zielteilnehmers, um die entschlüsselte Identität des Ursprungsteilnehmers zu erhalten,
eine Einrichtung zum Vergleichen der entschlüsselten Identität des Ursprungsteilnehmers mit der unverschlüsselt übertragenen Identität des Ursprungsteilnehmers,
eine Einrichtung zum Weiterverarbeiten einer vom Ursprungsteilnehmer empfangenen Nachricht bei Übereinstimmung der verglichenen Identitäten.

Über die Kommunikationseinrichtung wird der Ursprungsteilnehmer mit dem Kommunikationsnetz verbunden, so dass eine Verbindung sowohl zum Zielteilnehmer als auch zur Registrieungseinrichtung über das Kommunikationsnetz erfolgt. Alternativ kann die Kommunikationseinrichtung zwei separate Schnittstellen aufweisen, die den Ursprungsteilnehmer einmal mit dem Kommunikationsnetz und zum anderen mit der Registrierungseinrichtung vebindet.

Um eine gesicherte, vorzugsweise verschlüsselte Nachricht vom Ursprungsteilnehmer zum Zielteilnehmer übertragen zu können, weist die Registrierungeinrichtung weiterhin auf:
eine Einrichtung zum Erzeugen eines kryptografischen Schlüssels,
eine Einrichtung zum Verknüpfen des kryptografischen Schlüssels mit der Identität des Ursprungsteilnehmers,
wobei
die erste Verschlüsselungseinrichtung zum Verschlüsseln des von der Verknüpfungseinrichtung gelieferten Wertes mit dem individuellen Teilnehmerschlüssel des Zielteilnehmers ausgebildet und den ersten verschlüsselten Wert liefert,
eine zweite Verschlüsselungseinrichtung zum Erzeugen eines zweiten verschlüsselten Wertes durch Verschlüsseln des kryptografischen Schlüssels mit dem individuellen Teilnehmerschlüssel des Ursprungsteilnehmers,

wobei der Ursprungsteilnehmer folgende weitere Merkmale aufweist:
eine Einrichtung zum Entschlüsseln des zweiten verschlüsselten Wert mit seinem individuellen Teilnehmerschlüssel, um den kryptografischen Schlüssel zu gewinnen;
eine Einrichtung zum Sichern einer zu versendenden Nachricht unter Verwendung des kryptografischen Schlüssels,
wobei die Kommunikationseinrichtung (110, 115) zum Senden der gesicherten Nachricht, der Identität des Ursprungsteilnehmers und des ersten verschlüsselten Wertes zum Zielteilnehmer ausgebildet ist;
wobei die Zieleinrichtung folgende weitere Merkmale aufweist:
eine Entsicherungseinrichtung, beispielsweise eine Entschlüsselungseinrichtung, zum Entsichern der empfangenen Nachricht mit Hilfe des kryptografischen Schlüssel, wobei die Entschlüsselungseinrichtung zum Entschlüsseln des ersten verschlüsselten Wertes mit Hilfe dessen individuellen Teilnehmerschlüssel ausgebildet ist, um die entschlüsselte Identität des Ursprungsteilnehmers und den kryptografischen Schlüssel zu erhalten.

Die zeitlich begrenzte Nutzung des kryptografischen Schlüssels wird dadurch erreicht, dass
die Registrierungseinrichtung folgende weitere Merkmale aufweist:
eine Einrichtung zum Ermitteln des Zeitpunktes, zu dem der kryptografische Schlüssel erzeugt worden ist,
wobei die Verknüpfungseinrichtung zum Verknüpfen des kryptografischen Schlüssels mit der Identität des Ursprungsteilnehmers und dem Zeitpunkt ausgebildet ist,
wobei die wenigstens eine Registrierungseinrichtung, der Ursprungs- und/oder der Zielteilnehmer eine Einrichtung zum Berechnen des Ablaufs einer vorbestimmten Zeitspanne in

Bezug auf den ermittelten Zeitpunkt aufweisen.

Vorzugsweise weist der Zielteilnehmer eine Einrichtung zum Verwerfen einer empfangenen Nachricht auf. Diese Einrichtung spricht zweckmäßiger Weise auf den zeitlichen Ablauf der Nutzungsdauer des kryptografischen Schlüssels und/oder einer Nicht-Übereinstimmung zwischen der im Zielteilnehmer entschlüsselten Identität des Ursprungsteilnehmers und dessen unverschlüsselt empfangenen Identität an.

Fener kann die Registrierungseinrichtung eine Schnittstelle zum Verbinden mit wenigstens einer weiteren Registrierungseinrichtung und eine Einrichtung zum Suchen der Registrierungseinrichtung, die dem Zielteilnehmer zugeordnet ist, oder in der der Zielteilnehmer durch seine Identität registriert ist, aufweisen.

Das oben genannte Problem wird ebenfalls durch eine Registrierungseinrichtung, die zum Einsatz in dem oben umschriebenen Sicherheitssystem geeignet ist, gelöst.

Die Registrierungseinricht weist wenigstens eine
Teilnehmer-Anschlussschnittstelle,
eine Speichereinrichtung, in der wenigstens die Identität eines Teilnehmers gespeichert ist,
eine Einrichtung zum Erzeugen individueller Teilnehmerschlüssel unter Ansprechen auf die wenigstens eine gespeicherte Identität und zum Senden der individuellen Teilnehmerschlüssel zu den dazugehörenden Teilnehmern,
eine Einrichtung zum Vergleichen der von einem Ursprungs- und/oder Zielteilnehmer gesendeten Identität mit den gespeicherten Identitäten und
eine erste Einrichtung zum Verschlüsseln der Identität des

Ursprungsteilnehmers mit dem individuellen Teilnehmerschlüssel des Zielteilnehmers auf, so dass ein erster verschlüsselter Wert entsteht, der für den Ursprungsteilnehmer bestimmt ist.

Vorteilhafter Weise enthält die Registrierungseinrichtung eine Einrichtung zum Erzeugen eines kryptografischen Schlüssels, eine Einrichtung zum Verknüpfen des kryptografischen Schlüssels mit der Identität des Ursprungsteilnehmers, wobei die erste Verschlüsselungseinrichtung zum Verschlüsseln des von der Verknüpfungseinrichtung gelieferten Wertes mit dem individuellen Teilnehmerschlüssel des Zielteilnehmers ausgebildet und den ersten verschlüsselten Wert liefert, und
eine zweite Verschlüsselungseinrichtung zum Erzeugen eines zweiten verschlüsselten Wertes durch Verschlüsseln des kryptografischen Schlüssels mit dem individuellen Teilnehmerschlüssel des Ursprungsteilnehmers.

Die Registrierungseinrichtung kann zudem eine Einrichtung zum Ermitteln des Zeitpunktes aufweisen, zu dem der kryptografische Schlüssel (K_s) erzeugt worden ist. Die Verknüpfungseinrichtung ist dann zum Verknüpfen des kryptografischen Schlüssels mit der Identität des Ursprungsteilnehmers und dem Zeitpunkt ausgebildet ist.

Ferner kann die Registrierungseinrichtung eine Einrichtung zum Berechnen des Ablaufs einer vorbestimmten Zeitspanne in Bezug auf den ermittelten Zeitpunkt und
eine Einrichtung zum Sperren der Nutzung des kryptografischen Schlüssels aufweisen.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels in Verbindung mit den beiliegenden Zeichnungen erläutert. Es zeigen:

Fig. 1 in schematischer Darstellung das erfindungsgemäße Sicherheitssystem,

Fig. 2 das Blockschaltbild einer in Fig. 1 dargestellten Registrierungseinrichtung 30/40, in der die Erfindung verwirklicht ist,

Fig. 3 das Blockschaltbild des in Fig. 1 dargestellten Ursprungsteilnehmers, in der die Erfindung verwirklicht ist, und

Fig. 4 das Blockschaltbild des in Fig. 1 dargestellten Zielteilnehmers, in der die Erfindung verwirklicht ist.

Fig. 1 zeigt ein Sicherheitssystem, welches als Computernetz beispielsweise das öffentliche Internet 50 und zwei daran angeschlossene Computer 10 und 20 umfasst. Ferner gehören zum Sicherheitssystem zwei Registrierungseinrichtungen 30 und 40. Im vorliegenden Beispiel ist die Registrierungseinrichtung 30 mit dem Computer 10 verbunden, wohingegen die Registrierungseinrichtung 40 mit dem Computer 20 verbunden ist. Alternativ können die Registrierungseinrichtung 30, der Computer 10, die Registrierungseinrichtung 40 und der Computer 20 über das Intenet 50 miteinander verbunden sein. Selbstverständlich können mehrere Computer an das Internet angeschlossen, mehrere Registrierungseinrichtungen miteinander verbunden und mehrere Computer einer Registrierungseinrichtung zugeordnet sein. Die miteinander verbundenen Registrierungseinrichtungen 30 und 40 können Teil eines intelligenten Netzes sein, welches dem Internet übergeordnet ist. Für das vorliegende Beispiel sei angenommen, dass der Computer 10 als Ursprungsteilnehmer

einer Nachricht und der Computer 20 als Zielteilnehmer der Nachricht fungieren.

Der Aufbau der Registrierungseinrichtungen 30 und 40 ist in Fig. 2 gezeigt.

Die Registrierungseinrichtungen 30 und 40 weisen eine Schnittstelle 80 auf, über die sie mit dem Computer 10 bzw. mit dem Computer 20, in Fig. 1 auch als Teilnehmer A und Teilnehmer B dargestellt, kommunizieren können. Daten können zwischen der Registrierungseinrichtung 30 und dem Computer 10 bzw. zwischen der Registrierungseinrichtung 40 und dem Computer 20 verschlüsselt übertragen werden. Mit der Schnittstelle 80 ist ein Speicher 60 verbunden, in dem die Identität ID_A des Computers 10, beispielsweise eine E-mail-Adresse, die Nutzungsdauer n zur Nutzung eines kryptografischen Schlüssels K_s und die Teilnehmerschlüssel abgelegt werden können. Nur der besseren Darstellung wegen wurde der Speicher 60 durch zwei Einrichtungen, die jeweils mit dem Bezugszeichen 60 versehen sind, dargestellt. Ein Vergleicher 260 ist mit der Schnittstelle 80 und dem Speicher 60 verbunden, um die vom Computer 10 gelieferten Identitäten ID_A des Computers 10 und ID_B des Computers 20 mit den im Speicher 60 gespeicherten Identitäten vergleichen zu können. Eine Sucheinrichtung 250 ist mit einer Schnittstelle 100 und dem Vergleicher 260 verbunden, um für den Fall, dass die Identität ID_B des Zielcomputers 20 nicht im Speicher 60 abgelegt ist, die Registrierungseinrichtung, im vorliegenden Fall die Registrierungseinrichtung 40 zu suchen, in der die Identität ID_B des Computers 20 abgelegt ist. Eine Verknüpfungseinrichtung 190 ist eingangsseitig mit dem Speicher 60 und einem Schlüsselgenerator 180 und ausgangsseitig mit einer Verschlüsselungseinirchtung 200 verbunden. Der Schlüsselgenerator 180 ist mit einem

Zeitgeber 230 verbunden, der den Zeitpunkt des Erzeugens eines kryptografischen Schlüssels K_s ermittelt. Der Zeitgeber 230 kann mit einem Zeitablaufberechner 270 verbunden sein, der mit dem Speicher 60 verbunden ist, um feststellen zu können, zu welchem Zeitpunkt die Nutzungsdauer n des Schlüssels Ks verstrichen ist. Ferner ist ein Teilnehmerschlüssel-Generator 70 mit dem Speicher 60 und einer Verschlüsselungseinrichtung 205 verbunden. Der Teilnehmerschlüssel-Generator 70 erzeugt für jeden Computer, dessen Identität im Speicher 60 abgelegt ist, wenigstens einen individuellen Teilnehmerschlüssel. Im vorliegenden Beispiel wird ein Teilnehmerschlüssel K_A für den Computer 10 erzeugt, der zum Computer 10 über eine gesicherte Verbindung übertragen werden kann. In ähnlicher Weise erzeugt die Registrierungseinrichtung 40 einen Teilnehmerschlüssel K_B für den Computer 20, der wiederum über eine gesicherte Verbindung zum Computer 20 übertragen werden kann. Die Teilnehmerschlüssel werden in dem Speicher 60 abgelegt. Die Verschlüsselungseinrichtung 200 ist ferner mit dem Speicher 60 und der Schnittstelle 80 verbunden. Die Verschlüsselungseinrichtung 205 ist mit dem Teilnehmerschlüssel-Generator 70 und dem Schlüsselgenerator 180 verbunden. Die Schnittstelle 80 ist ferner mit der Schnittstelle 100 verbunden. Über jeweilige Schnittstellen 100 sind die Registrierungseinrichtungen 30 und 40 miteinander verbunden.

Fig. 3 zeigt schematisch den Sendeteil des Computers 10, wohingegen Fig. 4 schematisch den Empfangsteil des Computers 20 zeigt. Es ist offensichtlich, dass beide Computer 10 und 20 sowohl einen Sende- als auch einen Empfangsteil enthalten können. Die besondere Darstellung in Fig. 3 und 4 wurde nur gewählt, um den beispielhaften Einsatz des Computers 10 als Nachrichtensender und den

beispielhaften Einsatz des Computers 20 als Nachrichtenempfänger wiederzugeben.

Der Computer 10 ist über eine Schnittstelle 115 mit der Registrierungseinrichtung 30 und über eine Schnittstelle 110 mit dem Internet 50 verbunden. Der Computer 10 enthält eine Entschlüsselungseinrichtung 210, eine damit verbundene Verschlüsselungseinrichtung 230 zum Verschlüsseln einer zu versendenden Nachricht m und einen Schlüsselspeicher 220, der mit der Entschlüsselungseinrichtung und der Verschlüsselungseinrichtung 230 verbunden sein kann. Die Verschlüsselungseinrichtung 230 ist eine mögliche Realisierung einer Sicherungseinrichtung.

Wie Fig. 4 zeigt, weist der Computer 20 eine Schnittstelle 120 zur Verbindung mit dem Internet 50 und eine Schnittstelle 130 zur Kommunikation mit der Registrierungseinrichtung 40 auf. Mit der Schnittstelle 120 ist eine Entschlüsselungseinichtung 140 und ein Vergleicher 160 verbunden. Eine weitere Entschlüsselungseinrichtung 145 ist mit einem Entscheider 240, der Entschlüsselungseinrichtung 140, der Schnittstelle 120 und einem Display 170 zur Darstellung der entschlüsselten Nachricht m verbunden. Das Display 170 ist ferner mit dem Entscheider 240 und dem Vergleicher 160 verbunden. Ein Schlüsselspeicher 150 ist mit der Entschlüsselungseinrichtung 140 und der Schnittstelle 120 verbunden.

Nachfolgend wird die Funktionsweise des Sicherheitssystems näher erläutert.

Die Funktionsweise des Sicherheitssystems umfasst zwei Stufen, eine Registrierungsphase bei den

Registrierungseinrichtungen 30 und 40 und eine Betriebsphase.

Die Registrierungsphase beginnt damit, dass die Identität ID_A des Computers 10 in dem Speicher 60 der Registrierungseinrichtung 30 gespeichert wird. Der Teilnehmerschlüssel-Generator 70 erstellt daraufhin einen Teilnehmerschlüssel K_A für den Computer 10. Der Teilnehmerschlüssel K_A wird im Speicher 60 gespeichert und wird über die Schnittstelle 80 vorzugsweise verschlüsselt nur zum Computer 10 übertragen und dort im Schlüsselspeicher 220 abgelegt. In ähnlicher Weise wird die Identität ID_B des Computers 20 in dem Speicher der Registrierungseinrichtung 40 gespeichert. Der Teilnehmerschlüssel-Generator 70 der Registrierungseinrichtung 40 erstellt daraufhin einen Teilnehmerschlüssel K_B für den Computer 20. Der Teilnehmerschlüssel K_B wird in dem Speicher 60 der Registrierungseinrichtung 40 gespeichert und über die Schnittstelle 80 vorzugsweise verschlüsselt nur zum Computer 20 übertragen und dort in einem Schlüsselspeicher 150 abgelegt. Die Computern 10 und 20 können mit der Registrierungseinrichtung 30 bzw. 40 vereinbaren, welches Verschlüsselungsverfahren für die nachfolgende Betriebsphase verwendet wird. Wie bereits erwähnt, werden in den Registrierungseinrichtungen 30 und 40 die Identitäten der jeweils registrierten Computer, die Teilnehmerschlüssel und das Verschlüsselungsverfahren gespeichert.

Hinsichtlich der Betriebsphase sei nunmehr angenommen, dass der Computer 10 eine Nachricht m zum Computer 20 senden möchte.

Zunächst sendet der Computer 10 eine Anfrage an die Registrierungseinrichtung 30 unter Angabe seiner eigenen Identität ID_A und der Identität ID_B des Computers 20, um eine Verbindung über das Internet 50 zum Computer 20 zu erhalten. Die Identitäten der Computer können die e-mail Adressen sein. Es müssen genau dieselben Identitätsangaben verwendet werden, die bereits bei der Registrierung der Computers 10 und 20 in der Registrierungseinrichtung 30 bzw. 40 verwendet wurden.

Der Vergleicher 260 der Registrierungseinrichtung 30 prüft nach Erhalt der Identitäten ID_A und ID_B, ob die Identität ID_A des Computers 10 im Speicher 60 gespeichert ist. Ist der Computer 10 nicht registriert, wird die Anfrage hinsichtlich eines Verbindungswunsches zu Computer 20 verworfen und der Computer 10 erhält eine entsprechende Nachricht. Der Vergleicher 260 bestätigt jedoch im vorliegenden Fall, dass der Computer 10 in der Registrierungseinrichtung 30 registriert ist, und prüft weiter, ob auch der Computer 20 registriert ist, d. h. ob die Identität ID_B im Speicher 60 der Registrierungseinrichtung 30 enthalten ist. Dies ist im vorliegenden Beispiel nicht der Fall. Unter Ansprechen darauf veranlasst die Sucheinrichtung 250 der Registrierungseinrichtung 30 eine Suche nach der Registrierungseinrichtung in der der Computer 20 registriert ist. Hierbei kann die Sucheinrichtung 260 die angegebene Identität ID_B des Computers 20 verwenden, um die Registrierungseinrichtung 40 zu finden, in der der Computer 20 registriert ist. Bei der Suche werden die Identitäten ID_A und ID_B der Computer 10 und 20 zu den jeweiligen Regristrierungseinrichtung zur Prüfung auf Übereinstimmung mit den jeweils gespeicherten Identitäten übertragen.

Die Suche kann solange durchgeführt werden, bis die Registrierungseinrichtung, in der der Computer 20 registriert ist gefunden wird. Sobald die Registrierungseinrichtung 40 die Identitäten ID_A und ID_B von der Registrierungseinrichtung 30 erhält, prüft der Vergleicher 260 der Registrierungseinrichtung 40, ob die Identität ID_B im Speicher 60 abgelegt ist.

Da der Computer 20 in der Registrierungseinrichtung 40 registriert ist, erzeugt der Schlüsselgenerator 180 der Registrierungseinrichtung 40 einen Zufallsschlüssel K_s. Der Zeitgeber 230 der Registrierungseinrichtung 40 ermittelt einen Zeitstempel t, der dem Zeitpunkt der Erzeugung des Zufallsschlüssel entspricht. Der Zufallsschlüssel K_s wird jetzt mit der Identität ID_A des Computers 10 und dem Zeitstempel t durch einen Algorithmus in der Verknüpfungseinrichtung 190 der Registrierungseinrichtung 40 verknüpft. Der Algorithmus für die Verknüpfung ist dabei von untergeordneter Bedeutung und kann im einfachsten Falle aus einem Aneinanderfügen der Werte bestehen. Der so gebildete Verknüpfungswert kann in dem Speicher 60 der Registrierungseinrichtung 40 gespeichert werden. Der Verknüpfungswert wird in der Verschlüsselungseinrichtung 200 der Registrierungseinrichtung 40 mit Hilfe des Teilnehmerschlüssels K_B des Computers 20 verschlüsselt und ergibt den Wert r. Es gilt:

$$r = \text{Funktion E } (Ks \mid IDA \mid t, K_B)$$

Daraufhin wird sowohl der Wert r als auch der Zufallsschlüssel K_s und optional die im Speicher 60 abgelegt Nutzungsdauer n des Zufallsschlüssels K_s auf vertraulichem Wege, in der Regel verschlüsselt, an die Registrierungseinrichtung 30 gesendet. Hierbei ist

wesentlich, dass der Zufallsschlüssel K_s auf dem Übertragungsweg nicht ausgeforscht werden kann.

In der Verknüpfungseinrichtung 190 der Registrierungseinrichtung 30 wird der Zufallsschlüssel K_s mit der Nutzungszeit n verknüpft. In der Verschlüsselungseinrichtung 200 wird ein Wert s gebildet, indem der Ausgangswert der Verknüpfungseinrichtung 190 mit Hilfe des Teilnehmerschlüssels K_A des Computers 10 verschlüsselt wird. Es gilt:

$$s = \text{Funktion } E\ (Ks \mid n,\ K_A)$$

Die Werte r und s werden nun an den Computer 10 gesendet.

In der Entschlüsselungseinrichtung 210 des Computers 10 wird der Wert s mit Hilfe des Teilnehmerschlüssels K_A des Computers 10 entschlüsselt, um den Zufallsschlüssel K_s und die Nutzungsdauer n zu gewinnen. Die Nutzungsdauer n gibt an, wie lange der Zufallsschlüssel K_s verwendet werden kann. Es gilt:

$$K_S \mid t = \text{Funktion } D\ (s,\ K_A)$$

Nunmehr wird in der Verschlüsselungseinrichtung 230 die zu übertragende Nachricht m mit dem Zufallsschlüssel K_s verschlüsselt, wodurch der Wert v gebildet wird. Diese Sicherung kann, wie im Beispiel verwendet, durch eine Verschlüsselungsfunktion, eine schlüsselabhängige Hash-Funktion, einen verschlüsselten Hash-Wert oder durch "Message Authentication Code" MAC basierend auf dem Schlüssel K_s realisiert werden. Für die Verschlüsselung ist lediglich wichtig, dass die Verschlüsselungsfunktion von dem Schlüssel K_s abhängt und ohne Kenntnis des Schlüssels K_s invertiert werden kann.

Es gilt für den Wert v:

$$v = \text{Funktion } E\ (m,\ K_S)$$

Nunmehr wird die bearbeitete Nachricht v mit der unverschlüsselten Identität ID_A des sendenden Computers 10 und dem Wert r über das Internet 50 zum Computer 20 gesendet.

Der Computer 20 erhält die Informationen v, ID_A und r. Zunächst wird der Wert r mit dem im Teilnehmerschlüssel-Speicher 150 gespeicherten Teilnehmerschlüssel K_B in der Entschlüsselungseinrichtung 140 entschlüsselt. Es gilt:

$$K_S \mid ID_A \mid t = \text{Funktion } D\ (r,\ K_B)$$

Der entschlüsselte Wert von ID_A und der unverschlüsselt übertragene Wert von ID_A werden nun im Vergleicher 160 verglichen. Sind die Werte nicht identisch, wurde die Identität ID_A des Computers 10 manipuliert. Das Ergebnis wird dem Entscheider 240 zugeführt, der veranlasst, dass eine weitere Verarbeitung, zum Beispiel die Entschlüsselung der Nachricht m in der Entschlüsselungseinrichtung 145 nicht durchgeführt oder abgebrochen wird. Eine manipulierte Absenderidentität wurde somit entdeckt.

Stellt der Vergleicher 160 jedoch, wie im vorliegenden Beispiel eine Übereinstimmung der verglichenen Werte für die Identität ID_A fest, so überprüft optional der Entscheider 240 anhand der übertragenen Nutzungsdauer n und des ermittelten Zeitpunkts des Entstehens des Zufallsschlüssels K_s, ob die Nutzungsdauer n mit Bezug auf den ermittelten Zeitstempel t der Erstellung des Zufallsschlüssels K_s überschritten worden ist. Ist dies der Fall, wird die weitere Verarbeitung der verschlüsselten

Nachricht m durch den Entscheider 240 abgebrochen, weil der Schlüssel K_s zu alt ist.

Der Ablauf der Nutzungszeit n des Schlüssels K_s kann auch vom Zeitablauf-Berechner 270 der Registrierungseinrichtungen 30 und 40 festgestellt werden, woraufhin die jeweilige Registrierungseinrichtung die Nutzung des Zufallsschlüssels K_s sperrt und den Schlüssel löscht. Der Ablauf der Nutzungsdauer kann ferner im sendenden Computer 10 festgestellt werden.

Ist die Nutzungsdauer n noch nicht abgelaufen, wird die Entschlüsselungseinrichtung 145 vom Entscheider 240 freigegeben, auf die verschlüsselte Nachricht v die Funktion D mit dem Schlüssel K_S anzuwenden. Die Funktion D stellt eine Entschlüsselung, eine schlüsselabhängige Hash-Code-Überprüfung, eine Überprüfung eines verschlüsselten Hash-Code oder eine Überprüfung eines verschlüsselten MAC dar. Nach erfolgreicher Bearbeitung der Nachricht m, wobei m = Funktion D (v, K_S) kann die Nachricht zum Beispiel am Display 170 angezeigt, oder im Computer 20 abgespeichert werden.

Mit der Verschlüsselung der Nachricht m im Computer 10 kann verhindert werden, dass die Nachricht über das Internet 50 zum Computer 20 ausgeforscht oder manipuliert wird. Es könnte zum Beispiel eine beliebige Nachricht in eine gültige Kombination der Wert von ID_A und r eingeschleusst werden.

Bezugszeichenliste

10 Computer (Teilnehmer A)
20 Computer (Teilnehmer B)
30, 40 Registrierungseinrichtung
50 Internet (Kommunikationsnetz)
60 Speicher zum Ablegen der Identitäten, der Schlüssel, der Nutzungsdauer n
70 Teilnehmerschlüssel-Generator
80 Schnittstelle zur Verbindung mit Teilnehmer A oder B
90 Zeitgeber zum Ermitteln der Entstehungszeit des Schlüssels K_s
100 Schnittstelle zur Verbindung mit der Registrierungseinrichtung 30 oder 40
110 Schnittstelle zur Verbindung des Computers 10 mit dem Internet
115 Schnittstelle zur Verbindung des Computers 10 mit der Registrierungseinrichtung 30
120 Schnittstelle zur Verbindung des Computers 20 mit dem Internet
130 Schnittstelle zur Verbindung des Computers 20 mit der Registrierungseinrichtung 40
140 Entschlüsselunngseinrichtung zum Entschlüsseln des ersten Wertes r mit dem Teilnehmerschlüssel K_B
145 Entschlüsselungseinrichtung zum Entschlüssel einer verschlüsselten Nachricht mit Hilfe des Schlüssels K_s
150 Schlüsselspeicher zum Speichern der Schlüssel
160 Vergleicher zum Vergleichen der entschlüsselten ID_A mit der unverschlüsselt übertragenen ID_A
170 Display
180 Schlüsselgenerator zum Erzeugen eines Schlüssels K_s
190 Verknüpfungseinrichtung zum Verknüpfen der ID_A, des K_s und der Nutzungsdauer n

200 Verschlüsselungseinrichtung zum Verschlüsseln des Ergebnisses von der Verknüpfungseinrichtung mit K_B und zum Verschlüsseln der ID_A mit K_B

205 Verschlüsselungseinrichtung zum Verschlüsseln des Schlüssels K_s mit K_A

210 Entschlüsselungseinrichtung zum Entschlüsseln eines zweiten Wertes s mit Hilfe des Teilnehmerschlüssels $K_{A'}$, um den Schlüssel K_s zu gewinnen,

220 Schlüsselspeicher zum Speichern der Schlüssel

230 Verschlüsselungseinrichtung zum Verschlüsseln einer Nachricht m mit dem Schlüssel K_s

240 Entscheider zum Aktivieren oder Deaktivieren der Entschlüsselungseinrichtung 145 und des Displays 170

250 Sucheinrichtung

260 Vergleicher zum Vergleichen der empfangenen ID_A und ID_B mit dem Inhalt des Speichers 60

270 Zeitablauf-Berechner

Patentansprüche

1. Verfahren zum Erkennen einer unverfälschten Identität eines eine Nachricht sendenden Teilnehmers (10) bei einem diese Nachricht empfangenden Teilnehmer (20), wobei die Teilnehmer (10, 20) über ein Computernetz (50) miteinander verbunden werden können, mit folgenden Schritten:

   a) die individuellen Identitäten (ID_A, ID_B) mehrerer Teilnehmer (10, 20) werden in wenigstens einer Registierungseinrichtung (30, 40) gespeichert;

   b) für jeden Teilnehmer (10, 20) wird wenigstens ein individueller Teilnehmerschlüssel (K_A, K_B) erzeugt;

   c) vor Beginn der Übertragung einer Nachricht von einem Ursprungsteilnehmer (10) zu wenigstens einem Zielteilnehmer (20) wird geprüft, ob die individuellen Identitäten (ID_A, ID_B) der Ursprungs- und Zielteilnehmer (10, 20) in der wenigstens einen Registrierungseinrichtung (30, 40) gespeichert sind;

   d) wenn ja, wird die Identität (ID_A) des Ursprungsteilnehmers (10) mit dem individuellen Teilnehmerschlüssel (K_B) des Zielteilnehmers (20) verschlüsselt wird und ein erster verschlüsselter Wert (r) gebildet;

   e) der erste verschlüsselte Wert (r) wird zum Ursprungsteilnehmer (10) übertragen;

   f) eine Nachricht (m), die Identität (ID_A) des Ursprungsteilnehmers (10) und der erste verschlüsselte Wert (r) werden vom Urprungsteilnehmer (10) zum Zielteilnehmer (20) gesendet;

   g) der erste verschlüsselte Wert (r) wird mit dem individuellen Teilnehmerschlüssel (K_B) des Zielteilnehmers (20) entschlüsselt, um die

entschlüsselte Identität (ID_A) des Ursprungsteilnehmers (10) zu erhalten;

h) die entschlüsselte Identität (ID_A) des Ursprungsteilnehmers (10) wird mit der unverschlüsselt übertragenen Identität (ID_A) des Ursprungsteilnehmers (10) verglichen;

i) bei Übereinstimmung der verglichenen Identitäten wird die empfangene Nachricht zur Weiterverarbeitung weitergeleitet.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Schritte d) bis i) durch folgende Schritte ersetzt werden:

wenn die individuellen Identitäten (ID_A, ID_B) der Ursprungs- und Zielteilnehmer (10, 20) in der wenigstens einen Registrierungseinrichtung (30, 40) gespeichert sind, wird ein kryptografischer Schlüssel (K_s) erzeugt;

der kryptografische Schlüssel (K_s) wird mit der Identität (ID_A) des Ursprungsteilnehmers (10) verknüpft, wobei der erhaltende Wert dann mit dem individuellen Teilnehmerschlüssel (K_B) des Zielteilnehmers (20) verschlüsselt wird und den ersten verschlüsselten Wert (r) bildet;

der kryptografische Schlüssel (K_s) wird mit dem individuellen Teilnehmerschlüssel (K_A) des Ursprungsteilnehmers (10) verschlüsselt und bildet einen zweiten verschlüsselten Wert (s);

der erste und zweite verschlüsselte Wert (r, s) werden zum Ursprungsteilnehmer (10) übertragen;

der Ursprungsteilnehmer (10) entschlüsselt den zweiten verschlüsselten Wert (s) mit dem individuellen Teilnehmerschlüssel (K_A) des Ursprungsteilnehmers (10), um den kryptografischen Schlüssel (K_s) zu gewinnen;

die zu versendende Nachricht (m) wird unter Verwendung des kryptografischen Schlüssels (K_s) gesichert;
die gesicherte Nachricht (m), die Identität (ID_A) des Ursprungsteilnehmers (10) und der erste verschlüsselte Wert (r) werden vom Urprungsteilnehmer (10) zum Zielteilnehmer (20) gesendet;
der erste verschlüsselte Wert (r) wird mit dem individuellen Teilnehmerschlüssel (K_B) des Zielteilnehmers (20) entschlüsselt, um die entschlüsselte Identität (ID_A) des Ursprungsteilnehmers (10) und den kryptografischen Schlüssel (K_s) zu erhalten;
die entschlüsselte Identität (ID_A) des Ursprungsteilnehmers (10) wird mit der unverschlüsselt übertragenen Identität (ID_A) des Ursprungsteilnehmers (10) verglichen;
bei Übereinstimmung der verglichenen Identitäten wird die empfangene Nachricht mit dem kryptografischen Schlüssel (K_s) entsichert und zur Weiterverarbeitung weitergeleitet.

3. Verfahren nach Anspruch 2,
dadurch gekennzeichnet, dass
der Zeitpunkt der Erzeugung des kryptografischen Schlüssel (K_s) ermittelt und gespeichert wird, und dass die Nutzung des kryptografischen Schlüssels (K_s) durch den Ursprungs- und/oder Zielteilnehmer (10, 20) nach Ablauf einer vorbestimmten Zeitspanne gesperrt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet, dass
Schritt c) nach Anspruch 1 folgende Schritte umfasst:
vor Beginn der Übertragung einer Nachricht übersendet der Ursprungsteilnehmer (10) die individuellen Identitäten (ID_A, ID_B) der Ursprungs- und

Zielteilnehmer (10, 20) an die ihm zugeordnete Registrierungseinrichtung (30);
es wird geprüft, ob die individuellen Identitäten (ID_A, ID_B) des Ursprungs- und Zielteilnehmers (10, 20) in dieser Registrierungseinrichtung (30) gespeichert sind;
wenn nur die individuelle Identität (ID_A) des Ursprungteilnehmers (10) gespeichert ist, wird die Registrierungseinrichtung (40) gesucht, in der die Identität (ID_B) des Zielteilnehmers (20) gespeichert ist.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass
in den Teilnehmern (10, 20) vorbestimmte Identitäten anderer Teilnehmer gespeichert werden, deren gesendete Nachrichten bei einem entsprechenden Zielteilnehmer verworfen oder weitergeleitet werden.

6. Verfahren nach einem der Nasprüche 1 bis 5, dadurch gekennzeichnet, dass
die Identitäten Teilnehmeradressen, insbesondere E-mail-Adressen sind.

7. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass
der kryptografische Schlüssel (K_s) nach einem Zufallsalgorithmus erzeugt wird.

8. Sicherheitssystem zum Erkennen einer unverfälschten Identität eines eine Nachricht sendenden Ursprungsteilnehmers (10) bei einem diese Nachricht empfangenden Zielteilnehmer (20), insbesondere zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 7, umfassend
ein Kommunikationsnetz (50), insbesondere ein

öffentliches Computernetz,
wenigstens einen Ursprungs- und wenigstens einen Zielteilnehmer (10, 20), die an das Kommunikationsnetz (50) angeschlossen sind, und
wenigstens eine den Teilnehmern zugeordnete Registrierungseinrichtung (30, 40), wobei die Registrierungseinrichtung 30, 40) folgende Merkmale aufweist:
wenigstens eine Teilnehmer-Anschlussschnittstelle (80),
eine Speichereinrichtung (60), in der wenigstens die Identität eines Teilnehmers gespeichert ist,
eine Einrichtung (70) zum Erzeugen individueller Teilnehmerschlüssel (K_A, K_B) unter Ansprechen auf die wenigstens eine gespeicherte Identität,
eine Einrichtung (260) zum Vergleichen der von einem Ursprungs- und/oder Zielteilnehmer (10, 20) gesendeten Identität (ID_A, ID_B) mit den gespeicherten Identitäten,
eine erste Einrichtung (200) zum Verschlüsseln der Identität (ID_A) des Ursprungsteilnehmers (10) mit dem individuellen Teilnehmerschlüssel (K_B) des Zielteilnehmers (20), so dass ein erster verschlüsselter Wert (r) entsteht, der für den Ursprungsteilnehmer (10) bestimmt ist,
wobei der Ursprungsteilnehmer (10) folgende Merkmale aufweist:
eine Einrichtung (110, 115) zur Kommunikation mit der Registrierungseinrichtung (30) und dem Zielteilnehmer (20), wobei
der Zielteilnehmer (20) folgende Merkmale aufweist:
eine Einrichtung (140) zum Entschlüsseln des ersten verschlüsselte Wert (r) mit dem individuellen Teilnehmerschlüssel (K_B) des Zielteilnehmers (20), um die entschlüsselte Identität (ID_A) des Ursprungsteilnehmers (10) zu erhalten,
eine Einrichtung (160) zum Vergleichen der

entschlüsselten Identität (ID_A) des Ursprungsteilnehmers (10) mit der unverschlüsselt übertragenen Identität (ID_A) des Ursprungsteilnehmers (10),

eine Einrichtung zum Weiterverarbeiten (170) einer vom Ursprungsteilnehmer (10) empfangenen Nachricht bei Übereinstimmung der verglichenen Identitäten.

9. Sicherheitssystem nach Anspruch 8,
dadurch gekennzeichnet, dass
die Registrierungeinrichtung (30, 40) weiterhin aufweist:
eine Einrichtung (180) zum Erzeugen eines kryptografischen Schlüssels (K_s),
eine Einrichtung (190) zum Verknüpfen des kryptografischen Schlüssels (K_s) mit der Identität (ID_A) des Ursprungsteilnehmers (10), wobei
die erste Verschlüsselungseinrichtung (200) zum Verschlüsseln des von der Verknüpfungseinrichtung (190) gelieferten Wertes mit dem individuellen Teilnehmerschlüssel (K_B) des Zielteilnehmers (20) ausgebildet ist und den ersten verschlüsselten Wert (r) liefert,
eine zweite Verschlüsselungseinrichtung (205) zum Erzeugen eines zweiten verschlüsselten Wertes (s) durch Verschlüsseln des kryptografischen Schlüssels (K_s) mit dem individuellen Teilnehmerschlüssel (K_A) des Ursprungsteilnehmers (10),
wobei der Ursprungsteilnehmer (10) folgende weitere Merkmale aufweist:
eine Einrichtung (210) zum Entschlüsseln des zweiten verschlüsselten Wert (s) mit seinem individuellen Teilnehmerschlüssel (K_A), um den kryptografischen Schlüssel (K_s) zu gewinnen;
eine Einrichtung zum Sichern (230) einer zu

versendenden Nachricht (m) unter Verwendung des kryptografischen Schlüssels (K_s), wobei die Kommunikationseinrichtung (110, 115) zum Senden der gesicherten Nachricht (m), der Identität (ID_A) des Ursprungsteilnehmers (10) und des ersten verschlüsselten Wertes (r) zum Zielteilnehmer (20) ausgebildet ist;
wobei die Zieleinrichtung (20) folgende weitere Merkmale aufweist:
eine Einrichtung (145) zum Entsichern der empfangenen Nachricht mit Hilfe des kryptografischen Schlüssels (K_s), wobei die Entschlüsselungseinrichtung (140) zum Entschlüsseln des ersten verschlüsselten Wertes (r) mit Hilfe dessen individuellen Teilnehmerschlüssels (K_B) ausgebildet ist, um die entschlüsselte Identität (ID_A) des Ursprungsteilnehmers (10) und den kryptografischen Schlüssel (K_s) zu erhalten.

10. Sicherheitssystem nach Anspruch 9, dadurch gekennzeichnet, dass die Registrierungseinrichtung (30, 40) folgende weitere Merkmale aufweist:
eine Einrichtung (90) zum Ermitteln des Zeitpunktes (t), zu dem der kryptografische Schlüssel (K_s) erzeugt worden ist,
wobei die Verknüpfungseinrichtung (190) zum Verknüpfen des kryptografischen Schlüssels (K_s) mit der Identität (ID_A) des Ursprungsteilnehmers (10) und dem Zeitpunkt (t) ausgebildet ist,
wobei die wenigstens eine Registrierungseinrichtung (30, 40), der Ursprungs- und/oder der Zielteilnehmer (10, 20) eine Einrichtung (270) zum Berechnen des Ablaufs einer vorbestimmten Zeitspanne in Bezug auf den

ermittelten Zeitpunkt (t) aufweisen.

11. Sicherheitssystem nach Anspruch 10, dadurch gekennzeichnet, dass der Zielteilnehmer (20) eine Einrichtung (240) zum Verwerfen einer empfangenen Nachricht aufweist.

12. Sicherheitssystem nach einem der Ansprüche 8 bis 11, dadurch gekennzeichnet, dass die Registrierungseinrichtung (30) eine Schnittstelle (100) zum Verbinden mit wenigstens einer weiteren Registrierungseinrichtung (40) und eine Einrichtung (250) zum Suchen der Registrierungseinrichtung (40) aufweist, die dem Zielteilnehmer (20) zugeordnet ist.

13. Registrierungseinrichtung zum Einsatz in einem Sicherheitssystem nach einem der Ansprüche 8 bis 12, gekennzeichnet durch
wenigstens eine Teilnehmer-Anschlussschnittstelle (80),
eine Speichereinrichtung (40), in der wenigstens die Identität eines Teilnehmers gespeichert ist,
eine Einrichtung (70) zum Erzeugen individueller Teilnehmerschlüssel (K_A, K_B) unter Ansprechen auf die wenigstens eine gespeicherte Identität,
eine Einrichtung (260) zum Vergleichen der von einem Ursprungs- und/oder Zielteilnehmer (10, 20) gesendeten Identität (ID_A, ID_B) mit den gespeicherten Identitäten,
eine erste Einrichtung (200) zum Verschlüsseln der Identität (ID_A) des Ursprungsteilnehmers (10) mit dem individuellen Teilnehmerschlüssel (K_B) des Zielteilnehmers (20), so dass ein erster verschlüsselter Wert (r) entsteht, der für den Ursprungsteilnehmer bestimmt ist.

14. Registrierungseinrichtung nach Anspruch 13, gekennzeichnet durch
eine Einrichtung (180) zum Erzeugen eines kryptografischen Schlüssels (K_s),
eine Einrichtung (190) zum Verknüpfen des kryptografischen Schlüssels (K_s) mit der Identität (ID_A) des Ursprungsteilnehmers (10), wobei die erste Verschlüsselungseinrichtung (200) zum Verschlüsseln des von der Verknüpfungseinrichtung (190) gelieferten Wertes mit dem individuellen Teilnehmerschlüssel (K_B) des Zielteilnehmers (20) ausgebildet und den ersten verschlüsselten Wert (r) liefert,
eine zweite Verschlüsselungseinrichtung (205) zum Erzeugen eines zweiten verschlüsselten Wertes (s) durch Verschlüsseln des kryptografischen Schlüssels (K_s) mit dem individuellen Teilnehmerschlüssel (K_A) des Ursprungsteilnehmers (10).

15. Registrierungseinrichtung nach Anspruch 14, gekennzeichnet durch,
eine Einrichtung (230) zum Ermitteln des Zeitpunktes (t), zu dem der kryptografische Schlüssel (K_s) erzeugt worden ist,
wobei die Verknüpfungseinrichtung (190) zum Verknüpfen des kryptografischen Schlüssels (K_s) mit der Identität (ID_A) des Ursprungsteilnehmers (10) und dem Zeitpunkt (t) ausgebildet ist.

16. Registrierungseinrichtung nach Anspruch 15, gekennzeichnet durch
eine Einrichtung (270) zum Berechnen des Ablaufs einer vorbestimmten Zeitspanne in Bezug auf den ermittelten Zeitpunkt (t) und
eine Einrichtung zum Sperren der Nutzung des kryptografischen Schlüssels (K_s).

Fig. 1

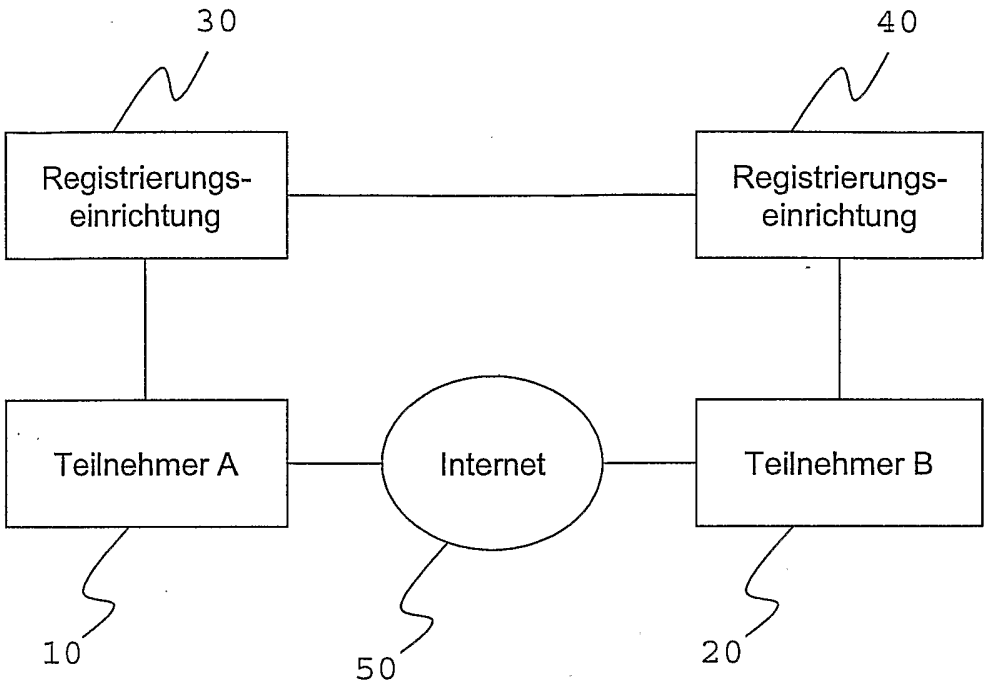

30
40
Registrierungs-einrichtung
Registrierungs-einrichtung
Teilnehmer A
Internet
Teilnehmer B
10
50
20

Fig. 2

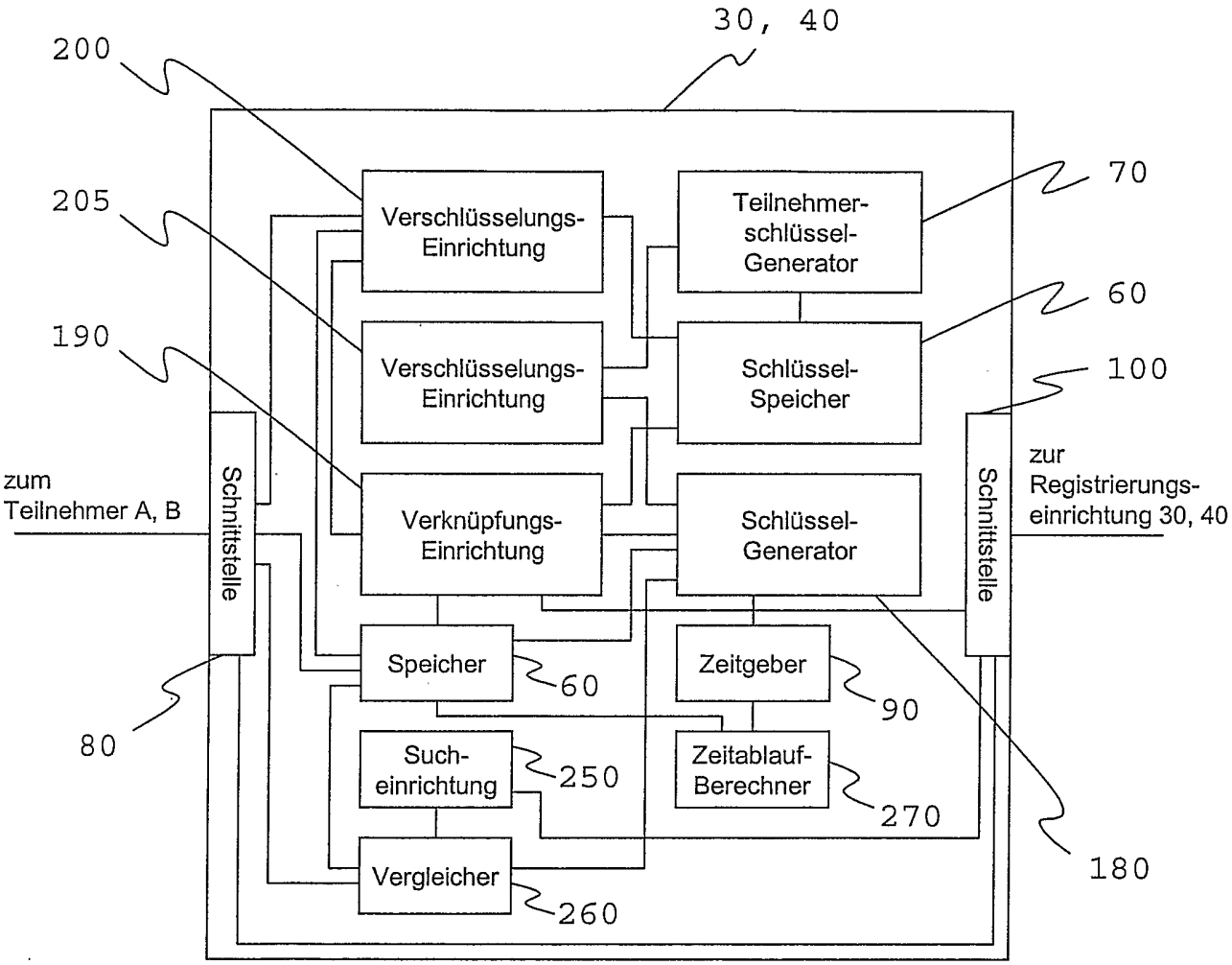

30, 40
200
205
190
70
60
100
Verschlüsselungs-Einrichtung
Verschlüsselungs-Einrichtung
Verknüpfungs-Einrichtung
Teilnehmer-schlüssel-Generator
Schlüssel-Speicher
Schlüssel-Generator
Schnittstelle
Schnittstelle
zum Teilnehmer A, B
zur Registrierungs-einrichtung 30, 40
Speicher
60
Zeitgeber
90
Such-einrichtung
250
Zeitablauf-Berechner
270
Vergleicher
260
80
180

Fig. 3

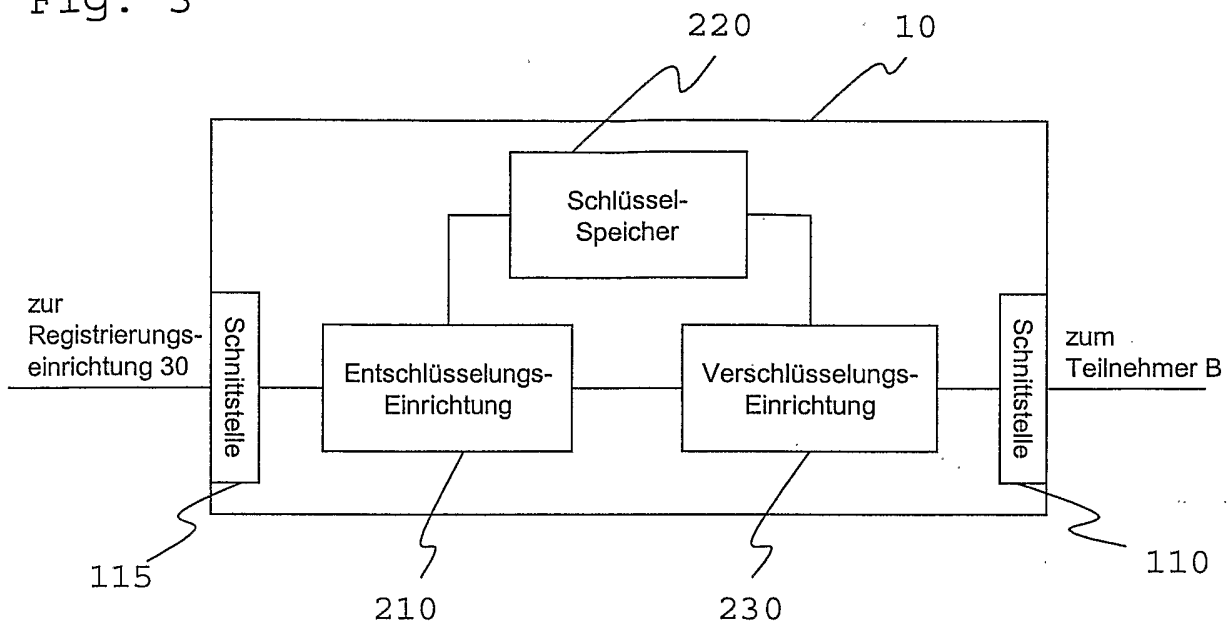
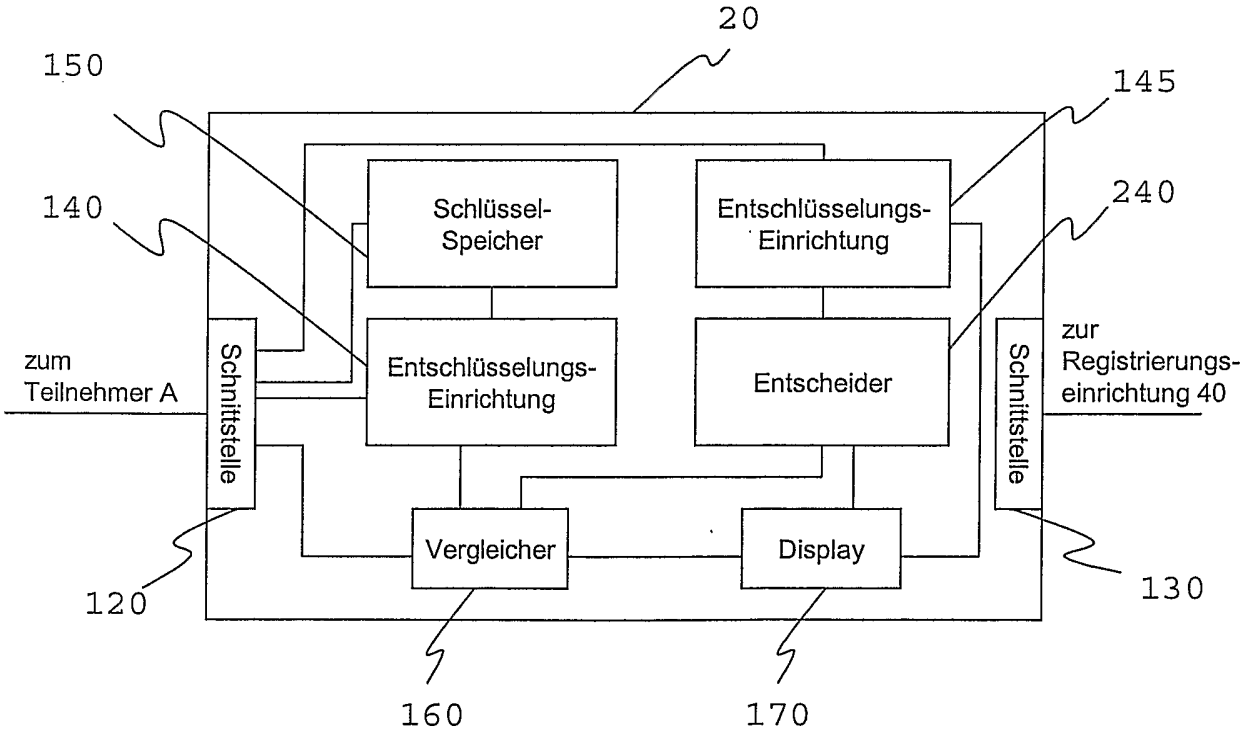

220
10
Schlüssel-
Speicher
zur
Registrierungs-
einrichtung 30
Schnittstelle
Entschlüsselungs-
Einrichtung
Verschlüsselungs-
Einrichtung
Schnittstelle
zum
Teilnehmer B
115
210
230
110

Fig. 4


20
150
145
140
240
Schlüssel-
Speicher
Entschlüsselungs-
Einrichtung
zum
Teilnehmer A
Schnittstelle
Entschlüsselungs-
Einrichtung
Entscheider
Schnittstelle
zur
Registrierungs-
einrichtung 40
Vergleicher
Display
120
130
160
170

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/007728

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 H04L12/58 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	S. KENT, BBN, IAB IRTF PSRG, IETF PEM: "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate -based Key Management" INTERNET ARTICLE, February 1993 (1993-02), XP015007209 page 4 - page 9 page 11	1-16
A	R. HOUSLEY, W. FORD, W. POLK, D. SOLO: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" INTERNET ARTICLE, January 1999 (1999-01), XP015008243 page 8 - page 12	1-16

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 October 2004	03/11/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kopp, K

1

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/007728

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 946 022 A (NIPPON TELEGRAPH & TELEPHONE) 29 September 1999 (1999-09-29) abstract paragraph '0005! paragraph '0010! - paragraph '0035! paragraph '0049! - paragraph '0050! paragraph '0142! - paragraph '0143! paragraph '0146! - paragraph '0158! figures 1,5	1-16
A	EP 1 162 781 A (TRW INC) 12 December 2001 (2001-12-12) paragraph '0003! paragraph '0005!	1-16

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/007728

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0946022 A	29-09-1999	EP 0946022 A2	29-09-1999
		JP 3449941 B2	22-09-2003
		JP 2000201169 A	18-07-2000
		JP 2004005690 A	08-01-2004
EP 1162781 A	12-12-2001	EP 1162779 A2	12-12-2001
		EP 1162780 A2	12-12-2001
		EP 1175037 A2	23-01-2002
		EP 1175038 A2	23-01-2002
		EP 1164745 A2	19-12-2001
		EP 1175039 A2	23-01-2002
		EP 1162781 A2	12-12-2001
		EP 1162807 A2	12-12-2001
		EP 1162782 A2	12-12-2001
		EP 1162783 A2	12-12-2001
		JP 2002082913 A	22-03-2002
		JP 2002064485 A	28-02-2002
		JP 2002049311 A	15-02-2002
		JP 2002033726 A	31-01-2002
		JP 2002057660 A	22-02-2002
		JP 2002135244 A	10-05-2002
		JP 2002057661 A	22-02-2002
		JP 2002135245 A	10-05-2002
		JP 2002124944 A	26-04-2002
		JP 2002123492 A	26-04-2002
		US 2002138724 A1	26-09-2002
		US 2003208690 A1	06-11-2003
		US 2002176582 A1	28-11-2002
		US 2002144111 A1	03-10-2002
		US 2002141592 A1	03-10-2002

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/007728

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/32 H04L12/58 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	S. KENT, BBN, IAB IRTF PSRG, IETF PEM: "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate -based Key Management" INTERNET ARTICLE, Februar 1993 (1993-02), XP015007209 Seite 4 - Seite 9 Seite 11 -----	1-16
A	R. HOUSLEY, W. FORD, W. POLK, D. SOLO: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" INTERNET ARTICLE, Januar 1999 (1999-01), XP015008243 Seite 8 - Seite 12 -----	1-16

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
26. Oktober 2004	03/11/2004

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Kopp, K

1

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/007728

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 946 022 A (NIPPON TELEGRAPH & TELEPHONE) 29. September 1999 (1999-09-29) Zusammenfassung Absatz '0005! Absatz '0010! - Absatz '0035! Absatz '0049! - Absatz '0050! Absatz '0142! - Absatz '0143! Absatz '0146! - Absatz '0158! Abbildungen 1,5	1-16
A	EP 1 162 781 A (TRW INC) 12. Dezember 2001 (2001-12-12) Absatz '0003! Absatz '0005!	1-16

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2004/007728

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0946022 A	29-09-1999	EP 0946022 A2	29-09-1999
		JP 3449941 B2	22-09-2003
		JP 2000201169 A	18-07-2000
		JP 2004005690 A	08-01-2004
EP 1162781 A	12-12-2001	EP 1162779 A2	12-12-2001
		EP 1162780 A2	12-12-2001
		EP 1175037 A2	23-01-2002
		EP 1175038 A2	23-01-2002
		EP 1164745 A2	19-12-2001
		EP 1175039 A2	23-01-2002
		EP 1162781 A2	12-12-2001
		EP 1162807 A2	12-12-2001
		EP 1162782 A2	12-12-2001
		EP 1162783 A2	12-12-2001
		JP 2002082913 A	22-03-2002
		JP 2002064485 A	28-02-2002
		JP 2002049311 A	15-02-2002
		JP 2002033726 A	31-01-2002
		JP 2002057660 A	22-02-2002
		JP 2002135244 A	10-05-2002
		JP 2002057661 A	22-02-2002
		JP 2002135245 A	10-05-2002
		JP 2002124944 A	26-04-2002
		JP 2002123492 A	26-04-2002
		US 2002138724 A1	26-09-2002
		US 2003208690 A1	06-11-2003
		US 2002176582 A1	28-11-2002
		US 2002144111 A1	03-10-2002
		US 2002141592 A1	03-10-2002