

(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
11. Dezember 2014 (11.12.2014)



(10) Internationale Veröffentlichungsnummer
WO 2014/195353 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2014/061569

(22) Internationales Anmeldedatum:
4. Juni 2014 (04.06.2014)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2013 105 740.3 4. Juni 2013 (04.06.2013) DE

(71) Anmelder: UNISCON UNIVERSAL IDENTITY
CONTROL GMBH [DE/DE]; Agnes-Pockels-Bogen 1,
80992 München (DE).

(72) Erfinder: JÄGER, Hubert; Habenschadenstr. 41a, 82049
Pullach (DE). MONITZER, Arnold; Wiener Str. 5, 82049
Pullach (DE). GEORGIEV, Vesko Mitkov; Apianstr. 7,
85774 Unterföhring (DE). KARATZAS, Christos;
Naupliastr. 33, 81547 München (DE). MODI, Jaymin;
Hötzlring 2, 81737 München (DE). NGUYEN, Dau
Khiem; Agnes-Bernauer-Str. 5, 80687 München (DE).
SPILLMANN, Dieter; Franziskanerstr. 36, 81669
München (DE).

(74) Anwalt: BETTINGER SCHNEIDER SCHRAMM;
Postfach 86 02 67, 81629 München (DE).

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

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,
GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ,
TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ,
RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY,
CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT,
LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE,
SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA,
GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR SECURING TELECOMMUNICATIONS TRAFFIC DATA

(54) Bezeichnung : VERFAHREN ZUR SICHERUNG VON TELEKOMMUNIKATIONSVERKEHRSDATEN

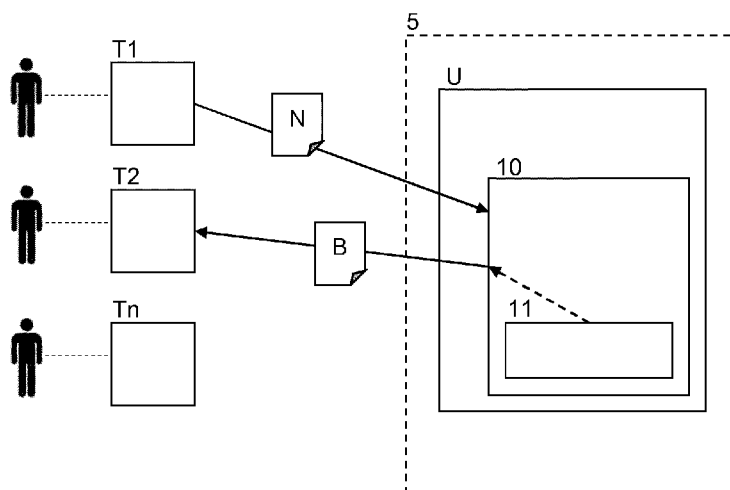


Fig. 1

(57) Abstract: The invention provides a method for securing telecommunications traffic data that accrue with the telecommunications service provider (5) of the telecommunications service when at least one telecommunications service (10) is used by a number of subscribers (T), wherein the telecommunications service is performed in a secure environment (U), the telecommunications service receives a message (N) from at least one first subscriber (T1) to the telecommunications service, said message being intended for at least one second subscriber (T2) to the telecommunications service, and the telecommunications service responds to the reception of the message (N) by sending a notification (B) to the at least one second subscriber, there being provision for a predetermined time offset (δT) between the reception of the message and the sending of the notification. In addition, a system for securing telecommunications traffic data is provided that is conditioned to perform the method according to the invention.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]

WO 2014/195353 A1

**Veröffentlicht:**

— mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

Bereitgestellt wird ein Verfahren zur Sicherung von Telekommunikationsverkehrsdaten, die bei einer Nutzung zumindest eines Telekommunikationsdienstes (10) von einer Anzahl von Teilnehmern (T) bei dem Telekommunikationsdienstleister (5) des Telekommunikationsdienstes anfallen, wobei der Telekommunikationsdienst in einer gesicherten Umgebung (U) ausgeführt wird, der Telekommunikationsdienst eine Nachricht (N) zumindest eines ersten Teilnehmers (T1) des Telekommunikationsdienstes entgegennimmt, die für zumindest einen zweiten Teilnehmer (T2) des Telekommunikationsdienstes bestimmt ist, und der Telekommunikationsdienst in Reaktion auf die Entgegennahme der Nachricht (N) eine Benachrichtigung (B) an den zumindest einen zweiten Teilnehmer sendet, wobei zwischen der Entgegennahme der Nachricht und dem Senden der Benachrichtigung ein vorbestimmter Zeitversatz (δt) vorgesehen wird. Ferner wird ein System zur Sicherung von Telekommunikationsverkehrsdaten bereitgestellt, das angepasst ist, das erfindungsgemäße Verfahren auszuführen.

VERFAHREN ZUR SICHERUNG VON TELEKOMMUNIKATIONSVERKEHRSDATEN

5

Gebiet der Erfindung

Die Erfindung betrifft ein System und ein Verfahren zur Sicherung von Telekom-
munikationsverkehrsdaten, die bei einer Nutzung eines Telekommunikationsdien-
10 tes von einer Anzahl von Teilnehmern des Telekommunikationsdienstes bei dem
Telekommunikationsdienstleister des Telekommunikationsdienstes anfallen.

15

Hintergrund der Erfindung

In einigen Ländern, etwa der Bundesrepublik Deutschland, werden bei einer Vor-
ratsdatenspeicherung personenbeziehbare bzw. personenbezogene Daten durch o-
der für sämtliche Stellen gespeichert, ohne dass die Daten aktuell benötigt werden.
20 Zweck einer solchen Vorratsdatenspeicherung soll eine verbesserte Möglichkeit der
Verhütung und Verfolgung von Straftaten sein. Hierzu müssen die Daten über einen
bestimmten Zeitraum gespeichert werden, damit sie beispielsweise für Strafverfol-
gungszwecke zur Verfügung stehen. Üblicherweise wird die Vorratsdatenspeiche-
rung von dem Anbieter bzw. Dienstleister eines Telekommunikationsdienstes
25 durchgeführt.

Um zu gewährleisten, dass der Anbieter des Telekommunikationsdienstes keine un-
berechtigten Zugriffe auf die Verkehrsdaten seiner Kunden hat, um etwa Persön-

- 2 -

lichkeitsprofile zu erstellen, ist es bekannt, die Verbindungsdaten in einer gesicherten Umgebung zu speichern und vor der Speicherung zu verschlüsseln. Die gesicherte Umgebung wird auch als versiegelte Infrastruktur bezeichnet. Die gesicherte Umgebung bzw. versiegelte Infrastruktur verhindert, dass weder der Betreiber der
5 Infrastruktur noch der den Telekommunikationsdienst anbietende Telekommunikationsdienstleister oder ein sonstiger Dritter auf diese Daten zugreifen kann. Weiter ist es bekannt, die Telekommunikationsdaten bzw. Verbindungsdaten mit zwei unterschiedlichen Verschlüsselungsschlüsseln zu verschlüsseln, wobei einer der beiden Schlüssel bei einer vertrauenswürdigen Instanz, etwa einem Notar hinterlegt
10 wird. Dadurch wird ein unberechtigter Zugriff auf die Verbindungs- bzw. Verkehrsdaten effizient verhindert, denn für den Zugriff ist in jedem Fall der bei der vertrauenswürdigen Instanz hinterlegte Schlüssel notwendig.

Um auch die zwischen den Teilnehmern eines Telekommunikationsdienstes ausgetauschten Daten, etwa elektronische Nachrichten oder elektronische Dokumente,
15 vor einem unberechtigten Zugriff des Telekommunikationsdienstleisters oder sonstiger Dritter zu verhindern, ist es bekannt, die von einem Teilnehmer empfangenen Daten ebenfalls zu verschlüsseln, sodass nur jene Teilnehmer Zugriff auf die Daten haben, für die die Daten bestimmt sind. Sowohl die Verschlüsselungs- als auch die
20 Entschlüsselungsschlüssel können in der vorstehend genannten gesicherten Umgebung gespeichert werden. Damit ist gewährleistet, dass weder der Telekommunikationsdienstleister noch sonstige Dritte weder auf die Verkehrsdaten noch auf die Nutzdaten Zugriff haben. Ein unberechtigtes Auswerten beispielsweise der Verkehrsdaten im Rahmen einer Rasterfahndung wird dadurch effektiv verhindert, so-
25 fern beispielsweise keine richterliche Anordnung vorliegt, die die Verwendung des bei einer vertrauenswürdigen Instanz, etwa einem Notar hinterlegten Schlüssel erlaubt.

Dieses aus dem Stand der Technik bekannte Verfahren zur Sicherung von Verkehrsdaten und Nutzdaten hat allerdings den Nachteil, dass, selbst wenn die Teilnehmer eines Telekommunikationsdienstes über gesicherte, etwa verschlüsselte
30

- 3 -

Kommunikationsverbindungen Daten untereinander austauschen, der Telekommunikationsdienstleister die Möglichkeit hat, anhand des Datenverkehrs die Information abzuleiten, wer mit wem kommuniziert. Diese Information kann der Telekommunikationsdienstleister selbst dann erhalten, wenn die Kommunikation zwischen den Teilnehmern und dem Telekommunikationsdienst verschlüsselt erfolgt, weil für die Information, wer mit wem kommuniziert, der Inhalt der zwischen den Teilnehmern ausgetauschten Daten nicht benötigt wird.

Dieses Problem tritt insbesondere dann auf, wenn ein Telekommunikationsdienst nach dem Erhalt einer Nachricht, etwa eines elektronischen Dokuments, von einem Teilnehmer jenen Teilnehmer, für den die Nachricht bestimmt ist, mit Hilfe einer weiteren Nachricht das Vorliegen einer für ihn bestimmten Nachricht signalisiert. Weil der Datenaustausch zwischen den Teilnehmern und dem Telekommunikationsdienst an sich für den Telekommunikationsdienstleister immer „sichtbar“ ist, kann der Telekommunikationsdienstleister aus der Tatsache, dass eine Nachricht für einen bestimmten Teilnehmer von einem Teilnehmer hinterlegt worden ist und der Teilnehmer, für den die Nachricht bestimmt ist, über das Vorliegen der Nachricht signalisiert wird, die Information erhalten, dass die beiden Teilnehmer miteinander kommunizieren, selbst wenn der Datenaustausch an sich verschlüsselt erfolgt und wenn der Teilnehmer, für den die Nachricht bestimmt ist, diese von dem Telekommunikationsdienst nicht anfordert.

Weil auch die Information, wer mit wem kommuniziert, zu den Telekommunikationsverkehrsdaten zählt, die für eine Rasterfahndung oder zur Erstellung von Persönlichkeitsprofilen herangezogen werden kann, sind die aus dem Stand der Technik bekannten Verfahren zur Vorratsdatenspeicherung trotz hoher Sicherheitsstandards nicht ausreichend geschützt bzw. gesichert, um die Möglichkeit einer unberechtigten Auswertung von Telekommunikationsverkehrsdaten effektiv zu verhindern.

Aufgabe der Erfindung

Aufgabe der Erfindung ist es daher, ein System und ein Verfahren zur Sicherung von Telekommunikationsverkehrsdaten, die bei einer Nutzung zumindest eines Telekommunikationsdienstes von einer Anzahl von Teilnehmern bei dem Telekommunikationsdienstleister des Telekommunikationsdienstes anfallen, bereitzustellen, welche einen unberechtigten Zugriff bzw. Missbrauch der Telekommunikationsverkehrsdaten effektiv und effizient verhindern.

10

Erfindungsgemäße Lösung

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren und ein System zur Sicherung von Telekommunikationsverkehrsdaten nach den unabhängigen Ansprüchen gelöst. Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung sind in den jeweiligen abhängigen Ansprüchen angegeben.

Bereitgestellt wird demnach ein Verfahren zur Sicherung von Telekommunikationsverkehrsdaten, die bei einer Nutzung zumindest eines Telekommunikationsdienstes von einer Anzahl von Teilnehmern bei dem Telekommunikationsdienstleister des Telekommunikationsdienstes anfallen, wobei der Telekommunikationsdienst eine Nachricht zumindest eines ersten Teilnehmers des Telekommunikationsdienstes entgegennimmt, die für zumindest einen zweiten Teilnehmer des Telekommunikationsdienstes bestimmt ist, und wobei der Telekommunikationsdienst in Reaktion auf die Entgegennahme der Nachricht eine Benachrichtigung an den zumindest einen zweiten Teilnehmer sendet, wobei zwischen der Entgegennahme der Nachricht und dem Senden der Benachrichtigung ein vorbestimmter Zeitversatz vorgesehen wird.

Vorteilhaft ist es, wenn der Telekommunikationsdienst in einer gesicherten Umgebung (versiegelte Infrastruktur) ausgeführt wird.

Dadurch, dass der Telekommunikationsdienst in einer gesicherten Umgebung bzw. versiegelten Infrastruktur ausgeführt wird, wird gewährleistet, dass der Telekommunikationsdienstleister des Telekommunikationsdienstes keinen Zugriff auf die
5 beim Telekommunikationsdienst anfallenden Daten hat. Um auch aus dem Datenverkehr zwischen den Teilnehmern und dem Telekommunikationsdienst keinerlei Informationen ableiten zu können, aus denen ermittelt werden kann, wer mit wem kommuniziert, ist der Zeitversatz zwischen der Entgegennahme einer Nachricht und dem Senden der Benachrichtigung vorgesehen. Dadurch wird verhindert, dass
10 anhand einer zeitlichen Korrelation zwischen der Entgegennahme einer Nachricht und dem Senden einer Benachrichtigung ermittelt werden kann, wer mit wem kommuniziert. Aufgrund des Zeitversatzes wird verhindert, dass eine Benachrichtigung einer entgegengenommenen Nachricht zugeordnet werden kann, sodass auch der Absender einer Nachricht nicht dem Empfänger der Benachrichtigung zuordenbar
15 ist.

Vorteilhaft ist es, wenn der Zeitversatz zwischen der Entgegennahme der Nachricht und dem Senden der Benachrichtigung in Abhängigkeit vom Datenverkehr pro Zeiteinheit zwischen den Teilnehmern des Telekommunikationsdienstes und dem
20 Telekommunikationsdienst gewählt wird. Damit kann der Zeitversatz bzw. das Senden der Benachrichtigungen an die Auslastung des Telekommunikationsdienstes vorzugsweise dynamisch angepasst werden.

Als besonders vorteilhaft hat sich herausgestellt, wenn der Zeitversatz bei einem
25 hohen Datenverkehr pro Zeiteinheit kleiner ist als bei einem geringen Datenverkehr pro Zeiteinheit.

Weil bei einem hohen Datenverkehr pro Zeiteinheit in der Regel von dem Telekommunikationsdienst Nachrichten von einer großen Anzahl von Teilnehmern entgegengenommen werden und damit auch Benachrichtigungen an eine große Anzahl
30 von Teilnehmern versendet werden, kann der Zeitversatz verkleinert werden ohne

dem Telekommunikationsdienstleister die Möglichkeit zu bieten, anhand einer zeitlichen Korrelation zwischen der Entgegennahme der Nachrichten und dem Senden der Benachrichtigungen die Information abzuleiten, wer mit wem kommuniziert. Bei einem geringen Datenverkehr pro Zeiteinheit nimmt der Telekommunikationsdienst in der Regel nur Nachrichten von einer geringen Anzahl von Teilnehmern entgegen und muss daher auch nur an eine geringe Anzahl von Teilnehmern eine entsprechende Benachrichtigung senden. Um auch für diesen Fall eine zeitliche Korrelation zwischen der Entgegennahme der Nachrichten und dem Senden der Benachrichtigungen zu verhindern, wird der Zeitversatz entsprechend vergrößert.

10

In einer Ausgestaltung der Erfindung wird der Zeitversatz zufällig aus einem Zeitversatzintervall ausgewählt. Der Zeitversatz kann für eine vorbestimmte Anzahl von zu sendenden Benachrichtigungen zufällig aus einem Zeitversatzintervall ausgewählt werden. Alternativ kann der Zeitversatz auch für jede zu sendende Benachrichtigung zufällig aus einem Zeitversatzintervall ausgewählt werden.

15

Dies hat den Vorteil, dass mit Hilfe einer zeitlichen Analyse des eingehenden und ausgehenden Datenverkehrs ein Ermitteln des aktuellen Zeitversatzes effektiv verhindert wird, was dem Telekommunikationsdienstleister ermöglichen würde, bei Kenntnis des aktuellen Zeitversatzes eine zeitliche Korrelation zwischen den entgegengenommenen Nachrichten und den gesendeten Benachrichtigungen herzustellen, aus denen der Telekommunikationsdienstleister die Information ableiten könnte, wer mit wem kommuniziert. Die Intervallgrenzen können festvorgegeben sein.

25

Vorteilhaft ist es aber, wenn die Intervallgrenzen des Zeitversatzintervalls in Abhängigkeit vom Datenverkehr pro Zeiteinheit zwischen den Teilnehmern und dem Telekommunikationsdienst gewählt werden. Damit wird nicht nur der Zeitversatz zufällig aus dem Zeitversatzintervall ausgewählt, sondern auch das Zeitversatzin-

tervall an den Datenverkehr angepasst, sodass für den Telekommunikationsdienstleister oder einem unberechtigten Dritten das Ermitteln des aktuellen Zeitversatzes noch weiter erschwert wird.

- 5 Der Zeitversatz (δt) kann für jeweils eine vorbestimmte Anzahl von Benachrichtigungen oder für jede Benachrichtigung verschieden gewählt werden.

In einer vorteilhaften Ausgestaltung der Erfindung umfasst der Datenverkehr pro Zeiteinheit die Anzahl der entgegengenommenen Nachrichten pro Zeiteinheit. Damit wird verhindert, dass bei einer geringen Anzahl von entgegengenommenen Nachrichten pro Zeiteinheit, die beispielsweise aufgrund von sehr großen Nachrichten einen hohen Datenverkehr verursachen, der Zeitversatz zu gering ausgewählt wird, was aufgrund der geringen Anzahl von entgegengenommenen Nachrichten und versendeten Benachrichtigungen eine zeitliche Korrelation zwischen den entgegengenommenen Nachrichten und den gesendeten Benachrichtigungen ermöglichen würde.

In einer Ausgestaltung der Erfindung kann der Telekommunikationsdienst einen Benachrichtigungsdienst umfassen, der die Benachrichtigung an den zumindest einen zweiten Teilnehmer erzeugt und das zeitversetzte Senden der erzeugten Benachrichtigung triggert, wobei der Zeitversatz von dem Benachrichtigungsdienst ermittelt wird.

In einer Ausgestaltung der Erfindung wird die Benachrichtigung an den zumindest einen zweiten Teilnehmer gesendet, wenn der zweite Teilnehmer an den Telekommunikationsdienst angemeldet ist. Es kann auch vorgesehen sein, dass an den zweiten Teilnehmer keine Benachrichtigung gesendet wird, wenn der Teilnehmer nicht an dem Telekommunikationsdienst angemeldet ist. Es kann vorgesehen sein, dem zweiten Teilnehmer auch dann keine Benachrichtigung zu senden, nachdem sich dieser zweite Teilnehmer an dem Telekommunikationsdienst angemeldet hat. Da-

mit wird eine noch bessere Dekorrelation erreicht, d.h., das Zuordnen einer Benachrichtigung zu einer entgegengenommenen Nachricht kann noch weiter erschwert werden.

- 5 Die Benachrichtigung kann Daten umfassen, die angepasst sind, an dem zweiten Teilnehmer ein akustisches und/oder visuelles Signal auszugeben, das das Vorliegen der Nachricht bei dem Telekommunikationsdienst signalisiert.

Die Benachrichtigung kann von jedem Teilnehmer identisch sein. In einer Ausgestaltung der Erfindung kann die Benachrichtigung unverschlüsselt gesendet werden. Weil die Benachrichtigung für jeden Teilnehmer identisch ist, kann sie auch unverschlüsselt gesendet werden, weil aus der Benachrichtigung keinerlei personenbezogenen Daten abgeleitet werden können. Das unverschlüsselte Versenden der Benachrichtigung hat zudem den Vorteil, dass auf Seiten des Telekommunikationsdienstes keine Verschlüsselung durchgeführt werden muss, was einen zusätzlichen Rechenaufwand bedeuten würde. Der Telekommunikationsdienst bzw. der Benachrichtigungsdienst, der die Benachrichtigung erzeugt und zeitversetzt sendet, kann so erheblich performanter und ressourcenschonender ausgeführt werden.

- 20 In einer Ausgestaltung der Erfindung kann die Nachricht auf Anforderung durch den zweiten Teilnehmer von dem Telekommunikationsdienst an den zweiten Teilnehmer übertragen werden. Weil die Benachrichtigung zeitversetzt zur Entgegennahme der Nachricht von dem ersten Teilnehmer an den zweiten Teilnehmer gesendet wird, kann auch aufgrund der Anforderung durch den zweiten Teilnehmer
25 die Nachricht an den zweiten Teilnehmer zu übertragen keine Information darüber abgeleitet werden, dass der erste Teilnehmer mit dem zweiten Teilnehmer kommuniziert.

Das erfindungsgemäße Verfahren zudem hat den Vorteil, dass die Kausalität zwischen den eingehenden Nachrichten und den zu versendeten Benachrichtigungen
30

- 9 -

aufgehoben wird, was ein Ableiten der Information wer mit wem kommuniziert unmöglich macht.

Die Übertragung der Nachricht von dem ersten Teilnehmer zu dem zweiten Teilnehmer (über den Telekommunikationsdienst) kann auf Basis einer Ende-zu-Ende-Verschlüsselung erfolgen, d.h., die Nachricht wird von dem ersten Teilnehmer verschlüsselt und von dem zweiten Teilnehmer entschlüsselt.

Die Nachricht kann homomorph verschlüsselt werden.

10

Des Weiteren wird durch die Erfindung ein System zur Sicherung von Telekommunikationsverkehrsdaten, die bei einer Nutzung zumindest eines Telekommunikationsdienstes von einer Anzahl von Teilnehmern bei den Telekommunikationsdienstleister des Telekommunikationsdienstes anfallen, bereitgestellt, wobei der Telekommunikationsdienst angepasst ist, eine Nachricht, die für einen zweiten Teilnehmer bestimmt ist, von zumindest einem ersten Teilnehmer entgegenzunehmen und in Reaktion auf die Entgegennahme der Nachricht eine Benachrichtigung an den zumindest einen zweiten Teilnehmer zu senden, wobei zwischen der Entgegennahme der Nachricht und dem Senden der Benachrichtigung ein vorbestimmter Zeitversatz vorgesehen ist.

20

Es hat sich als vorteilhaft herausgestellt, wenn das System eine gesicherte Umgebung umfasst, in der der Telekommunikationsdienst ausführbar ist.

Der Telekommunikationsdienst kann angepasst sein, den Zeitversatz zwischen der Entgegennahme der Nachricht und dem Senden der Benachrichtigung in Abhängigkeit vom Datenverkehr pro Zeiteinheit zwischen den Teilnehmern und dem Telekommunikationsdienst zu wählen.

Der Telekommunikationsdienst kann einen Benachrichtigungsdienst umfassen, der angepasst ist, die Benachrichtigung an den zumindest einen zweiten Teilnehmer zu

30

- 10 -

erzeugen und das zeitversetzte Senden der erzeugten Benachrichtigung zu triggern, wobei der Zeitversatz von dem Benachrichtigungsdienst ermittelt wird.

5 Ferner kann das erfindungsgemäße System weiter angepasst sein, ein erfindungsgemäßes Verfahren auszuführen.

Kurzbeschreibung der Erfindung

10 Einzelheiten und Merkmale der Erfindung sowie konkrete Ausführungsbeispiele der Erfindung ergeben sich aus der nachfolgenden Beschreibung in Verbindung mit der Zeichnung. Es zeigt:

15 Fig. 1 ein erfindungsgemäßes System zur Sicherung von Telekommunikationsverkehrsdaten zur Erläuterung des erfindungsgemäßen Verfahrens zur Sicherung der Telekommunikationsverkehrsdaten;

Fig. 2 den zeitlichen Ablauf zwischen dem Empfang einer Nachricht und dem Senden einer Benachrichtigung; und

20 Fig. 3 zwei Varianten für die erfindungsgemäße Auswahl eines Zeitversatzes in Abhängigkeit vom Datenverkehr.

Detaillierte Beschreibung der Erfindung

25 Mi dem erfindungsgemäßen System und dem erfindungsgemäßen Verfahren werden sowohl ein adäquater Datenschutz als auch hinreichend gute Möglichkeiten zur Datenauswertung, etwa zu Ermittlungszwecken, ermöglicht. Ein Missbrauch der gespeicherten Daten, insbesondere der Telekommunikationsverkehrsdaten wird effektiv vermieden, wobei insbesondere aus dem Datenverkehr keine Information ab-
30 geleitet werden kann, wer mit wem kommuniziert.

Fig. 1 zeigt ein erfindungsgemäßes System zur Sicherung von Telekommunikationsverkehrsdaten, die bei einer Nutzung eines Telekommunikationsdienstes 10 von einer Anzahl von Teilnehmern T1 bis Tn anfallen.

5

Ein Telekommunikationsdienstleister 5 stellt einen Telekommunikationsdienst 10 bereit, der in einer gesicherten Umgebung U ausgeführt wird. Durch den Telekommunikationsdienst 10 kann beispielsweise eine Nachrichtenbox bereitgestellt werden, in die für die Nachrichtenbox zugelassene Teilnehmer Nachrichten für andere Teilnehmer hinterlegen können. Eine Nachricht kann beispielsweise direkt in der Nachrichtenbox erzeugt werden oder über ein Kommunikationsnetzwerk in der Nachrichtenbox abgelegt werden. Eine Nachricht kann hier beispielsweise ein elektronisches Dokument oder dergleichen sein.

10

Bei dem in Fig. 1 gezeigten Beispiel wird eine Nachricht N, etwa ein elektronisches Dokument von einem ersten Teilnehmer T1 an den Telekommunikationsdienst 10 übertragen und dort beispielsweise in einer entsprechenden Nachrichtenbox abgelegt. Nach Erhalt der Nachricht N erzeugt der Telekommunikationsdienst 10 in der gesicherten Umgebung U eine Benachrichtigung B und sendet diese über ein Kommunikationsnetzwerk an den zweiten Teilnehmer T2. Mit der Benachrichtigung B wird der zweite Teilnehmer T2 darüber informiert, dass der erste Teilnehmer T1 eine Nachricht N für ihn in der Nachrichtenbox des Telekommunikationsdienstes 10 hinterlegt hat.

20

In einer Ausgestaltung der Erfindung umfasst der Telekommunikationsdienst 10 einen Benachrichtigungsdienst 11, der für das Erzeugen der Benachrichtigung an den zweiten Teilnehmer T2 und für das Senden der Benachrichtigung zuständig ist.

25

Sämtliche bei dem Telekommunikationsdienstleister 5 anfallenden Daten, d.h. Verkehrsdaten und Nutzdaten werden in der gesicherten Umgebung U gespeichert und gegebenenfalls verarbeitet. Wie Eingangs erläutert, können sowohl die Nutzdaten

30

als auch die Verkehrsdaten verschlüsselt, vorzugsweise doppelt verschlüsselt in der gesicherten Umgebung U gespeichert werden. Durch die doppelte Verschlüsselung ist gewährleistet, dass der Telekommunikationsdienstleister 5 keinen Zugriff auf die Nutz- und Verkehrsdaten erhält. Das Verschlüsseln bzw. doppelte Verschlüsseln der Daten wird vorzugsweise innerhalb der gesicherten Umgebung U durchgeführt, wobei auch die hierfür benötigten Schlüssel in der gesicherten Umgebung U erzeugt, gespeichert und verwaltet werden. Die gesicherte Umgebung U wird auch als versiegelte Infrastruktur bezeichnet und verhindert, dass weder der Betreiber der Infrastruktur noch der Telekommunikationsdienstleister bzw. Telekommunikationsdienstleister 5 während der Verarbeitung der Daten auf diese zugreifen kann.

Hierzu kann die gesicherte Umgebung U eine in Fig. 1 nicht gezeigte Einrichtung zum Erzeugen der benötigten kryptographischen Schlüssel umfassen. Um zu verhindern, dass die von dem Telekommunikationsdienstleister 5 in der gesicherten Umgebung U verschlüsselten Verbindungsdaten bzw. Nutzdaten ohne Weiteres von diesem mit Hilfe der entsprechenden Entschlüsselungs-Schlüssel wieder entschlüsselt werden können, ist es vorteilhaft, die verschlüsselten Daten mit einem weiteren Verschlüsselungsschlüssel nochmals zu verschlüsseln und die so doppelt verschlüsselten Daten in einer Speichereinrichtung der gesicherten Umgebung U abzulegen. Der zweite Verschlüsselungsschlüssel kann einer vertrauenswürdigen Instanz, etwa einem Notar, übergeben werden, der diesen nur auf eine richterliche Anordnung hin herausgeben kann.

Die gesicherte Umgebung U bzw. die versiegelte Infrastruktur kann eine Anzahl redundanter und verteilter Rechnerressourcen umfassen, welche jeweils eine Anzahl sogenannter Trusted Plattform Module (TPM), Leistungsschalter zur Unterbrechung der Stromversorgung der gesamten Rechnerressourcen, elektronmechanische Schlösser, eine Anzahl von Sensoren, mit denen der Zugang zu den Rechnerressourcen überwacht werden kann, umfassen können. In einer Ausgestaltung der Erfindung können die Rechnerressourcen Speichereinrichtungen aufweisen, in

denen die kryptographischen Schlüssel gespeichert werden, wobei in einer Ausgestaltung der Erfindung die kryptographischen Schlüssel ausschließlich in flüchtigen Speichermedien gespeichert werden, sodass nach einer Unterbrechung der Stromversorgung die gespeicherten Schlüssel gelöscht werden. Das Löschen der kryptographischen Schlüssel kann etwa dann erforderlich sein, wenn sich jemand unbefugt Zutritt bzw. Zugang zu einer Rechnerressource verschafft. Damit die Schlüssel wieder hergestellt werden können, ist es vorteilhaft, wenn die kryptographischen Schlüssel über eine Synchronisationseinrichtung mit einer weiteren Speichereinrichtung zum Speichern kryptographischer Schlüssel synchronisiert werden.

10

Die Rechnerressourcen können mit einer sogenannten Versiegelungsüberwachungseinrichtung (Sealing Control) verbunden sein, welche die elektromechanischen Komponenten überwacht. Stellt die Versiegelungsüberwachungseinrichtung einen unbefugten Zugang zu einer Rechnerressource fest, kann sie die sofortige Synchronisierung sämtlicher in der Rechnerressource gespeicherten Schlüssel veranlassen und nach Beendigung der Synchronisation die Stromversorgung zu der kompromittierten Rechnerressource unterbrechen. Damit ist gewährleistet, dass sich aus einer kompromittierten Rechnerressource keine Entschlüsselungsschlüssel mehr herstellen lassen können.

20

Die Rechnerressourcen können ferner mit einer sogenannten Cloud Control gekoppelt sein, die vorgesehen sein kann, den Datenaustausch mit einem oder mehreren Teilnehmer T abzuwickeln. Die Cloud Control kann ebenfalls mit der Versiegelungsüberwachungseinrichtung gekoppelt sein, sodass die Versiegelungsüberwachungseinrichtung auch bei einem festgestellten Einbruch über ein Kommunikationsnetzwerk entsprechende Maßnahmen einleiten kann.

Die Teilnehmer T1 bis Tn des Telekommunikationsdienstes 10 können Smartphones, Tablet-PCs, herkömmliche Computer oder dergleichen sein, wobei in dem in Fig. 1 gezeigten Beispiel ein Teilnehmer jeweils einem Nutzer zugeordnet ist. Wie

30

- 14 -

aus Fig. 1 ersichtlich ist, wird zwischen den Teilnehmern T1 und T2 und dem Telekommunikationsdienst 10 eine Datenübertragung abgewickelt, wobei Daten von dem ersten Teilnehmer T1 an den Telekommunikationsdienst 10 und Daten von dem Telekommunikationsdienst 10 an den zweiten Teilnehmer T2 übertragen werden, d.h. dass Daten von außerhalb der gesicherten Umgebung U zu dem Telekommunikationsdienst 10 gelangen bzw. Daten von dem Telekommunikationsdienst 10 aus der gesicherten Umgebung U heraus zu einem zweiten Teilnehmer T2 gelangen.

10 Auch wenn die Datenübertragung zwischen den beiden Teilnehmern T1, T2 und dem Telekommunikationsdienst 10 verschlüsselt abgewickelt wird, erhält der Telekommunikationsdienstleister 5 die Information, dass die Teilnehmer T1 und T2 an einer (gemeinsamen) Kommunikation beteiligt sind. Um zu verhindern, dass der Telekommunikationsdienstleister alleine aufgrund des Datenverkehrs (ohne hierfür
15 den Inhalt der gesendeten bzw. empfangenen Daten kennen zu müssen) die Information erhält, dass der erste Teilnehmer T1 mit dem zweiten Teilnehmer T2 kommuniziert, ist es erfindungsgemäß vorgesehen, dass die Benachrichtigung B von dem Telekommunikationsdienst 10 bzw. von dem Benachrichtigungsdienst 11 erzeugt wird und zeitversetzt an den zweiten Teilnehmer T2 gesendet bzw. übertragen
20 wird. Durch das zeitversetzte Senden der Benachrichtigung B wird erreicht, dass der Telekommunikationsdienstleister 5 anhand des Datenverkehrs keinerlei Zuordnung zwischen der empfangenen Nachricht N und der gesendeten Benachrichtigung B vornehmen kann und daher aus den Verkehrsdaten auch die Information, dass der Teilnehmer T1 mit dem Teilnehmer T2 kommuniziert, nicht ableiten kann. Durch
25 das Vorsehen eines Zeitversatzes zwischen der Entgegennahme der Nachricht N und dem Senden der Benachrichtigung B werden diese von außerhalb der gesicherten Umgebung U zugänglichen Verkehrsdaten „verschleiert“, sodass weder für den Telekommunikationsdienstleister 5 noch für einen unberechtigten Dritten erkennbar ist, wer mit wem und wie häufig kommuniziert.

In einer Ausgestaltung der Erfindung kann auch die Benachrichtigung B verschlüsselt werden bzw. verschlüsselt übertragen werden. Dies ist insbesondere dann vorteilhaft, wenn dem Empfänger der Nachricht N mit der Bestätigungsnachricht B mitgeteilt werden soll, wer die Nachricht N für ihn beispielsweise in einer Nachrichtenbox hinterlegt hat oder um welchen Inhalt es sich bei der in der Nachrichtenbox hinterlegten Nachricht handelt.

Als besonders vorteilhaft hat es sich jedoch herausgestellt, wenn mit der Benachrichtigung B lediglich die Information an den Empfänger bzw. an den zweiten Teilnehmer T2 übertragen wird, dass eine Nachricht für ihn bei dem Telekommunikationsdienstleister 5 hinterlegt wurde. Wenn mit der Benachrichtigung B nur die Information übertragen wird, dass eine Nachricht hinterlegt wurde, kann die Benachrichtigung B für sämtliche Teilnehmer des Telekommunikationsdienstes identisch sein, sodass auf eine Verschlüsselung bzw. auf eine verschlüsselte Übertragung der Benachrichtigung B verzichtet werden kann. Damit kann die Last des Systems auf Seiten des Telekommunikationsdienstleisters für das Erzeugen und Versenden der Benachrichtigungen erheblich reduziert bzw. minimiert werden.

In einer Ausgestaltung der Erfindung ist es ausreichend, wenn die Nutzdaten der Benachrichtigung B lediglich eine Länge von einem Bit aufweisen, denn zum Zwecke der Signalisierung des zweiten Teilnehmers T2, dass irgendeine Nachricht für ihn beim Telekommunikationsdienstleister hinterlegt wurde, ist ein Bit ausreichend. Damit kann das Datenvolumen für die Übertragung der Benachrichtigungen B an die Teilnehmer des Telekommunikationsdienstes reduziert bzw. minimiert werden.

Nach Erhalt der Benachrichtigung B kann der zweite Teilnehmer T2 die für ihn bestimmte Nachricht N von dem Telekommunikationsdienstleister anfordern. Die Kommunikation zwischen dem ersten Teilnehmer T1 und dem zweiten Teilnehmer T2 kann dabei auf Basis einer Ende-zu-Ende-Verschlüsselung erfolgen, d.h., der

erste Teilnehmer verschlüsselt die Nachricht und der zweite Teilnehmer entschlüsselt die Nachricht N. Zum Verschlüsseln der Nachricht kann ein homomorphes Verschlüsselungsverfahren verwendet werden. Dadurch kann z.B. der Telekommunikationsdienst Operation auf der Nachricht durchführen, ohne die Nachricht selbst
5 entschlüsseln zu müssen. Das Ergebnis der Operation liegt dann ebenfalls in verschlüsselter Form vor.

Fig. 2 zeigt den zeitlichen Verlauf des Empfangs einer Nachricht und des Sendens einer Benachrichtigung.

10

Zum Zeitpunkt t_1 empfängt der Telekommunikationsdienst des Telekommunikationsdienstleisters eine Nachricht von einem ersten Teilnehmer. Nach dem Empfang der Nachricht erzeugt der Telekommunikationsdienst bzw. der Benachrichtigungsdienst eine Benachrichtigung für den Teilnehmer, für den die empfangene Nachricht
15 bestimmt ist, und sendet die Benachrichtigung an diesen Teilnehmer, wobei zwischen der Entgegennahme der Nachricht zum Zeitpunkt t_1 und dem Senden der Benachrichtigung ein vorbestimmter Zeitversatz δt vorgesehen wird. D.h., die Benachrichtigung wird zum Zeitpunkt $t_1 + \delta t$ an den zweiten Teilnehmer gesendet.

20 Im einfachsten Fall der Erfindung kann ein konstanter Zeitversatz δt für alle zu versendenden Benachrichtigungen verwendet werden. Ein solcher konstanter Zeitversatz hat allerdings den Nachteil, dass dieser gegebenenfalls anhand einer Analyse des Datenverkehrs zwischen den Teilnehmern und dem Telekommunikationsdienst ermittelt werden kann, sodass bei Kenntnis des Zeitversatzes δt wieder eine
25 Zuordnung einer Benachrichtigung B zu einer empfangenen Nachricht N möglich wird. Um dies zu verhindern, kann es erfindungsgemäß vorgesehen sein, einen dynamischen Zeitversatz vorzusehen, der sich nach einer bestimmten Anzahl von Benachrichtigungen – im besten Fall nach jeder Benachrichtigung – ändert. Damit wird das Ermitteln eines Zeitversatzes durch Analyse des Datenverkehrs einerseits
30 erheblich erschwert und andererseits kann ein ermittelter Zeitversatz lediglich für einige in der Vergangenheit versendete Benachrichtigungen herangezogen werden,

um die Benachrichtigungen korrekt den jeweiligen empfangenen Benachrichtigungen zuordnen zu können, wohingegen ein so ermittelter Zeitversatz für eine derartige Zuordnung von Benachrichtigungen zu Nachrichten für zukünftig verschickte Benachrichtigungen bzw. empfangenen Nachrichten wertlos ist, weil sich der aktuelle Zeitversatz bis dahin bereits geändert hat.

Eine solche Dynamik des Zeitversatzes δt lässt sich beispielsweise dadurch erreichen, indem der Zeitversatz δt in Abhängigkeit vom Datenverkehr pro Zeiteinheit zwischen den Teilnehmern und dem Telekommunikationsdienst gewählt wird.

10

Beispiele für die Auswahl eines Zeitversatzes δt in Abhängigkeit vom Datenverkehr pro Zeiteinheit sind in Fig. 3 gezeigt.

Bei den in **Fig. 3** gezeigten Beispielen ist der Zeitversatz bei einem hohen Datenverkehr pro Zeiteinheit kleiner als bei einem geringen Datenverkehr pro Zeiteinheit d.h., dass bei einem hohen Datenverkehr ein geringerer Zeitversatz δt gewählt werden kann, als bei einem geringeren Datenverkehr, denn ein hoher Datenverkehr geht in der Regel mit einer großen Anzahl von Nachrichten einer großen Anzahl von Teilnehmern einher, sodass bereits aufgrund der großen Anzahl von versendenden Benachrichtigungen eine Zuordnung einer versendeten Benachrichtigung zu einer empfangenen Nachricht erschwert wird.

Bei dem in Fig. 3a gezeigten Beispiel ist der Zeitversatz δt nicht linear von dem Datenverkehr abhängig, während bei dem in Fig. 3b gezeigten Beispiel der Zeitversatz δt linear von dem Datenverkehr abhängig ist. Selbstverständlich können auch andere als die in Fig. 3a und Fig. 3b gezeigten Abhängigkeiten zwischen dem Zeitversatz δt und dem Datenverkehr gewählt werden.

In einer Ausgestaltung der Erfindung kann der Datenverkehr pro Zeiteinheit die Anzahl der entgegengenommenen Nachrichten N pro Zeiteinheit umfassen.

Um eine noch bessere Dynamik des ausgewählten Zeitversatzes δt zu erreichen, kann es vorgesehen sein, wenn der für das Versenden einer Benachrichtigung benötigte Zeitversatz δt zufällig aus einem Zeitversatzintervall ausgewählt wird. Hierbei kann der Zeitversatz δt für eine bestimmte Anzahl von zu versendenden Benachrichtigungen aus dem Zeitversatzintervall ausgewählt werden. Alternativ kann
5 der Zeitversatz δt für jede einzelne zu versendende Benachrichtigung zufällig aus dem Zeitversatzintervall ausgewählt werden. Damit wird erreicht, dass selbst bei einer umfassenden Analyse des Datenverkehrs zwischen den Teilnehmern und dem Telekommunikationsdienst keinerlei Rückschlüsse über die Zuordnung der Benachrichtigungen zu den empfangenen Nachrichten möglich ist, weil einerseits je-
10 der Zeitversatz einer bestimmten Zufälligkeit unterliegt und weil andererseits aufgrund der zufälligen Auswahl der Zeitversätze für die zu versendenden Benachrichtigungen die Reihenfolge der versendeten Benachrichtigungen nicht mehr der Reihenfolge der eingegangenen Nachrichten entspricht.

15 Die Zufallskomponente bei der zufälligen Auswahl des Zeitversatzes aus einem Zeitversatzintervall kann noch weiter verbessert werden, indem die Intervallgrenzen des Zeitversatzintervalls in Abhängigkeit vom Datenverkehr pro Zeiteinheit zwischen den Teilnehmern und dem Telekommunikationsdienst gewählt werden. Dadurch wird gewährleistet, dass bei einem großen Datenverkehr kleine Zeitversätze δt zufällig aus dem Zeitversatzintervall ausgewählt werden und bei einem ge-
20 ringen Datenverkehr größere Zeitversätze δt aus dem Zeitversatzintervall ausgewählt werden.

25 In einer Ausgestaltung der Erfindung können zusätzlich bzw. alternativ zu den vorstehend genannten Maßnahmen für die Auswahl eines Zeitversatzes die erzeugten Benachrichtigungen zufällig in eine Benachrichtigungswarteschlange eingereiht werden, sodass die Reihenfolge der zu versendenden Benachrichtigungen nicht mehr der Reihenfolge der empfangenen Nachrichten entspricht. Bei Verwendung
30 einer solchen Warteschlange, in der die zu versendenden Benachrichtigungen zufällig eingereiht werden, kann auf die zufällige Auswahl eines Zeitversatzes aus

- 19 -

einem Zeitversatzintervall auch verzichtet werden, denn aufgrund der zufälligen Einreihung der Benachrichtigungen in die Warteschlange ist auch bei einem konstanten Zeitversatz gewährleistet, dass eine gesendete Benachrichtigung nicht korrekt einer empfangenen Nachricht zugeordnet werden kann.

Bezugszeichen:

	5	Telekommunikationsdienstleister
	10	Telekommunikationsdienst
5	11	Benachrichtigungsdienst
	δt	Zeitversatz zwischen Datenempfang und Senden der Benachrichtigung
	B	Benachrichtigung zwischen Telekommunikationsdienst und Teilnehmer
	D	Daten der Benachrichtigung
10	N	Nachricht zwischen Teilnehmer und Telekommunikationsdienst
	T	Teilnehmer
	T1	erster Teilnehmer
	T2	zweiter Teilnehmer
	U	gesicherte Umgebung

Ansprüche

5

1. Verfahren zur Sicherung von Telekommunikationsverkehrsdaten, die bei einer Nutzung zumindest eines Telekommunikationsdienstes (10) von einer Anzahl von Teilnehmern (T) bei dem Telekommunikationsdienstleister (5) des Telekommunikationsdienstes anfallen, wobei

10

- der Telekommunikationsdienst zumindest eine Nachricht (N) zumindest eines ersten Teilnehmers (T1) des Telekommunikationsdienstes entgegennimmt, die für zumindest einen zweiten Teilnehmer (T2) des Telekommunikationsdienstes bestimmt ist, und

15

- der Telekommunikationsdienst in Reaktion auf die Entgegennahme einer Nachricht (N) eine Benachrichtigung (B) an den zumindest einen zweiten Teilnehmer sendet, wobei zwischen der Entgegennahme jeder Nachricht und dem Senden der entsprechenden Benachrichtigung jeweils ein Zeitversatz (δt) vorgesehen wird.

20

2. Verfahren nach Anspruch 1, wobei der Zeitversatz (δt) zwischen der Entgegennahme der Nachricht (N) und dem Senden der Benachrichtigung (B) in Abhängigkeit vom Datenverkehr pro Zeiteinheit zwischen den Teilnehmern (T) und dem Telekommunikationsdienst gewählt wird.

25

3. Verfahren nach Anspruch 2, wobei der Zeitversatz (δt) bei einem hohen Datenverkehr pro Zeiteinheit kleiner ist als bei einem geringen Datenverkehr pro Zeiteinheit.

4. Verfahren nach einem der Ansprüche 2 oder 3, wobei der Zeitversatz (δt) zufällig aus einem Zeitversatzintervall ausgewählt wird.
5. Verfahren nach Anspruch 5, wobei die Intervallgrenzen des Zeitversatzintervalls in Abhängigkeit vom Datenverkehr pro Zeiteinheit zwischen den Teilnehmern (T) und dem Telekommunikationsdienst gewählt werden.
6. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Zeitversatz (δt) für jeweils eine vorbestimmte Anzahl von Benachrichtigungen oder für jede Benachrichtigung verschieden gewählt wird.
7. Verfahren nach einem der Ansprüche 2 bis 7, wobei der Datenverkehr pro Zeiteinheit die Anzahl der entgegengenommenen Nachrichten (N) pro Zeiteinheit umfasst.
8. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Telekommunikationsdienst (10) einen Benachrichtigungsdienst (11) umfasst, der die Benachrichtigung (B) an den zumindest einen zweiten Teilnehmer (T2) erzeugt und das zeitversetzte Senden der erzeugten Benachrichtigung triggert, wobei der Zeitversatz (δt) von dem Benachrichtigungsdienst ermittelt wird und wobei der Telekommunikationsdienst in einer gesicherten Umgebung (U) ausgeführt wird.
9. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Benachrichtigung (B) nicht an den zweiten Teilnehmer (T2) gesendet wird, wenn der zweite Teilnehmer nicht an dem Telekommunikationsdienst (10) angemeldet ist.
10. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Benachrichtigung (B) Daten (D) umfasst, die angepasst sind, an dem zweiten Teilnehmer (T2) ein akustisches und/oder visuelles Signal auszugeben, das das Vorliegen der Nachricht (N) signalisiert.

11. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Benachrichtigung (B) für jeden Teilnehmer (T) identisch ist.
12. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Benachrichtigung (B) unverschlüsselt gesendet wird.
- 5 13. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachricht (N) auf Anforderung durch den zweiten Teilnehmer (T2) von dem Telekommunikationsdienst (10) an den zweiten Teilnehmer übertragen wird.
14. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Übertragung der Nachricht (N) von dem ersten Teilnehmer (T1) zu dem zweiten
10 Teilnehmer (T2) auf Basis einer Ende-zu-Ende-Verschlüsselung erfolgt, wobei die Nachricht vorzugsweise homomorph verschlüsselt wird.
15. System zur Sicherung von Telekommunikationsverkehrsdaten, die bei einer Nutzung zumindest eines Telekommunikationsdienstes (10) von einer Anzahl von Teilnehmern (T) bei dem Telekommunikationsdienstleister (5) des
15 Telekommunikationsdienstes anfallen, wobei der Telekommunikationsdienst angepasst ist eine Nachricht (N), die für einen zweiten Teilnehmer (T2) bestimmt ist, von zumindest einem ersten Teilnehmer (T1) entgegenzunehmen und in Reaktion auf die Entgegennahme der Nachricht (N) eine Benachrichtigung (B) an den zumindest einen zweiten Teilnehmer zu
20 senden, wobei zwischen der Entgegennahme der Nachricht und dem Senden der Benachrichtigung ein vorbestimmter Zeitversatz (δt) vorgesehen ist.
16. System nach Anspruch 15, wobei der Telekommunikationsdienst angepasst ist den Zeitversatz (δt) zwischen der Entgegennahme der Nachricht (N) und dem Senden der Benachrichtigung (B) in Abhängigkeit vom Datenverkehr
25 pro Zeiteinheit zwischen den Teilnehmern (T) und dem Telekommunikationsdienst zu wählen.

17. System nach einem der Ansprüche 15 oder 16, wobei der Telekommunikationsdienst (10) einen Benachrichtigungsdienst (11) umfasst, der angepasst ist die Benachrichtigung (B) an den zumindest einen zweiten Teilnehmer (T2) zu erzeugen und das zeitversetzte Senden der erzeugten Benachrichtigung zu triggern, wobei der Zeitversatz (δt) von dem Benachrichtigungsdienst ermittelt wird und wobei das System eine gesicherte Umgebung umfasst, in der der Telekommunikationsdienst ausführbar ist,.
- 5
18. System nach einem der Ansprüche 15 bis 17, wobei das System weiter angepasst ist ein Verfahren nach einem der Ansprüche 1 bis 14 auszuführen.

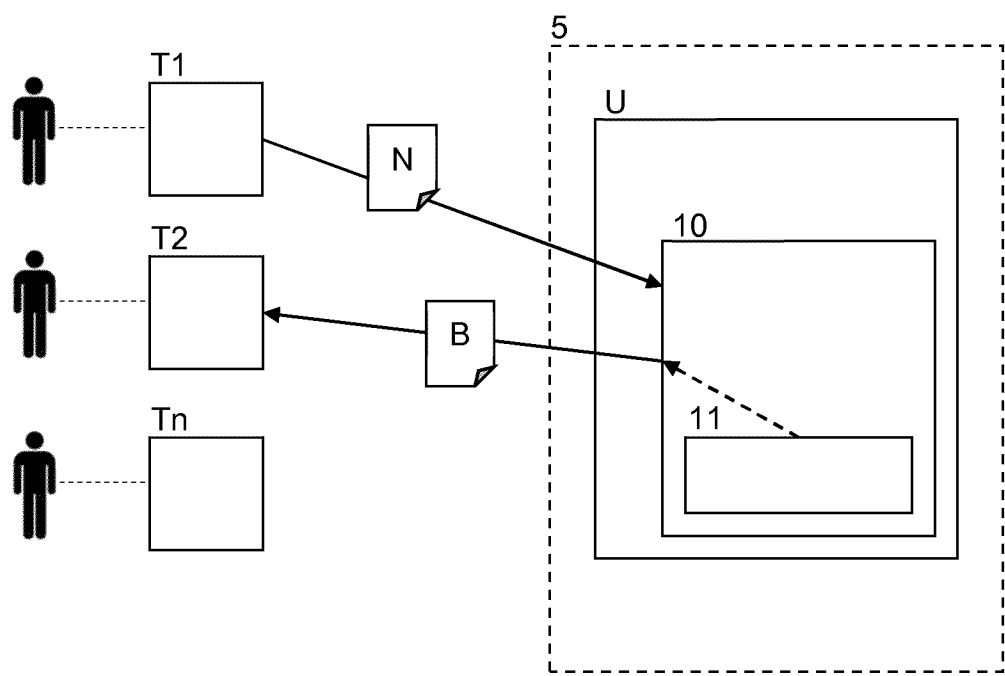


Fig. 1

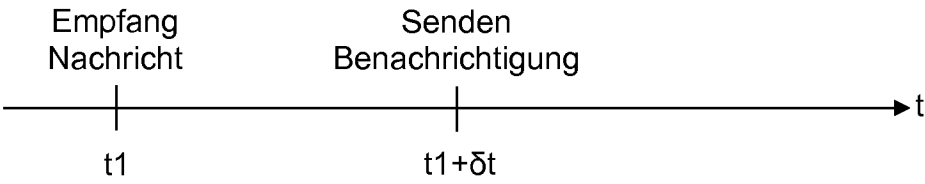


Fig. 2

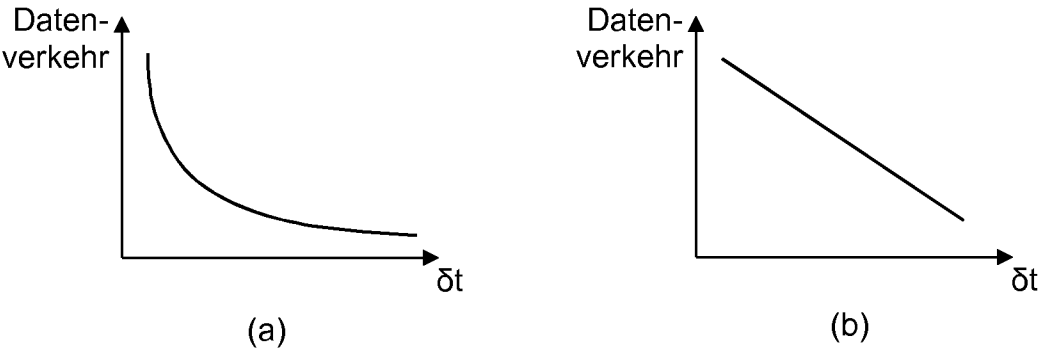


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2014/061569

A. CLASSIFICATION OF SUBJECT MATTER
 INV. H04L29/06
 ADD.

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)
 H04L

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 practicable, search terms used)

EPO-Internal, INSPEC, COMPENDEX, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/076089 A1 (FONSECA ARNOLDO MEDEIROS [US]) 7 April 2005 (2005-04-07) paragraph [0087] - paragraph [0088] paragraph [0117] - paragraph [0120] paragraph [0123] - paragraph [0131] paragraph [0136] - paragraph [0143] paragraph [0155] - paragraph [0156]; claims 1-3,13-20; figures 1,2,4.1.A-8 -----	1-18
X	US 2006/023727 A1 (GEORGE DAVID A [US] ET AL) 2 February 2006 (2006-02-02) paragraph [0004] - paragraph [0006] paragraph [0024] - paragraph [0029]; claims 1-3,15-17,24,29; figures 1,3 -----	1,15
A	-/--	2-14, 16-18



Further documents are listed in the continuation of Box C.



See patent family 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 application or patent 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

29 August 2014

Date of mailing of the international search report

04/09/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Schwibinger, Hans

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2014/061569

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 2 523 421 A1 (HUAWEI TECH CO LTD [CN]) 14 November 2012 (2012-11-14) paragraph [0025] - paragraph [0027] paragraph [0036] - paragraph [0038] paragraph [0052] - paragraph [0054]; claims 1,18,25,46-48; figure 2 -----	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2014/061569

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005076089	A1	07-04-2005	NONE

US 2006023727	A1	02-02-2006	NONE

EP 2523421	A1	14-11-2012	CN 102137105 A 27-07-2011
			EP 2523421 A1 14-11-2012
			US 2013160140 A1 20-06-2013
			WO 2012122920 A1 20-09-2012

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

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, INSPEC, COMPENDEX, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2005/076089 A1 (FONSECA ARNOLDO MEDEIROS [US]) 7. April 2005 (2005-04-07) Absatz [0087] - Absatz [0088] Absatz [0117] - Absatz [0120] Absatz [0123] - Absatz [0131] Absatz [0136] - Absatz [0143] Absatz [0155] - Absatz [0156]; Ansprüche 1-3,13-20; Abbildungen 1,2,4.1.A-8 -----	1-18
X	US 2006/023727 A1 (GEORGE DAVID A [US] ET AL) 2. Februar 2006 (2006-02-02) Absatz [0004] - Absatz [0006] Absatz [0024] - Absatz [0029]; Ansprüche 1-3,15-17,24,29; Abbildungen 1,3 -----	1,15
A	-/--	2-14, 16-18

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ 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" frühere Anmeldung oder Patent, die bzw. 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 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

29. August 2014

Absendedatum des internationalen Recherchenberichts

04/09/2014

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Schwibinger, Hans

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 2 523 421 A1 (HUAWEI TECH CO LTD [CN]) 14. November 2012 (2012-11-14) Absatz [0025] - Absatz [0027] Absatz [0036] - Absatz [0038] Absatz [0052] - Absatz [0054]; Ansprüche 1,18,25,46-48; Abbildung 2 -----	1-18

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2014/061569

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2005076089	A1	07-04-2005	KEINE
US 2006023727	A1	02-02-2006	KEINE
EP 2523421	A1	14-11-2012	CN 102137105 A 27-07-2011
			EP 2523421 A1 14-11-2012
			US 2013160140 A1 20-06-2013
			WO 2012122920 A1 20-09-2012