(19) DANMARK

(10) DK/EP 3005645 T3

(12) Oversættelse af europæisk patentskrift

Patent- og Varemærkestyrelsen

(51) Int.Cl.: *H 04 L 29/06 (2006.01)*

(45) Oversættelsen bekendtgjort den: **2018-05-28**

(80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2018-02-14**

(86) Europæisk ansøgning nr.: **14729275.9**

(86) Europæisk indleveringsdag: **2014-06-04**

(87) Den europæiske ansøgnings publiceringsdag: **2016-04-13**

(86) International ansøgning nr.: **EP2014061569**

(87) Internationalt publikationsnr.: **WO2014195353**

(30) Prioritet: **2013-06-04 DE 102013105740**

(84) Designerede stater: **AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**

(73) Patenthaver: **Uniscon universal identity control GmbH, Agnes-Pockels-Bogen 1, 80992 München, Tyskland**

(72) Opfinder: **JÄGER, Hubert, Habenschadenstr. 41a, 82049 Pullach, Tyskland**
MODI, Jaymin, Hötzlring 2, 81737 München, Tyskland
NGUYEN, Dau Khiem, Agnes-Bernauer-Str. 5, 80687 München, Tyskland
KARATZAS, Christos, Profiti Ilia 11, Palaia Fokea, PO 19013, Athen, Grækenland
SPILLMANN, Dieter, 4124 Valerie Dr., Campbell, CA 95008, USA
MONITZER, Arnold, Wittelsbacherring 30, 85229 Markt Indersdorf, Tyskland
GEORGIEV, Vesko Mitkov, 120 Republican, ¤ 503, Seattle, WA 98109, USA

(74) Fuldmægtig i Danmark: **Budde Schou A/S, Hausergade 3, 1128 København K, Danmark**

(54) Benævnelse: **Fremgangsmåde til sikring af data i telekommunikationstrafik**

(56) Fremdragne publikationer:
EP-A1- 2 523 421
US-A1- 2005 076 089
US-A1- 2006 023 727

Description

Field of the Invention

The present invention relates to a system and a method for securing telecommunication traffic data which, when a telecommunication service is used by a given number of users of said telecommunication service, is generated at the telecommunication service provider of said telecommunication service.

Background of the invention

In some countries, such as in the Federal Republic of Germany, data that could be related to individual persons or person-related data is preventively stored within the frame of a telecommunications data retention scheme by or on behalf of all kinds of authorities, although these data are not currently needed for any specific purpose. Such preventive data retention is aimed at enhancing the possibilities of preventing and prosecuting criminal offences. To this end, the data needs to be stored for a certain period of time so as to be available for purposes of criminal prosecution. Usually, such preventive data retention is carried out by the supplier or service provider of a telecommunication service.

In order to make sure that the supplier of the telecommunication service is prevented from illegally accessing the traffic data of his clients in order to create personality profiles, for example, it is known to store the communication data in a secured environment and to encrypt it prior to storage. The secured environment is also referred to as a sealed infrastructure. This secured environment or sealed infrastructure prevents the provider of said infrastructure as well as the telecommunication service provider who provides the telecommunication service and any other third party from accessing this data. It is further known to encrypt the telecommunications data or communication data using two different encryption keys, with one of the two keys being deposited at a trusted party such as a notary public. Thus it is possible to efficiently prevent any unauthorised access to communication data or traffic data, since the key deposited at the trusted party is a prerequisite for any data access whatsoever.

In order to also protect the data exchanged between the users of a telecommunication service, such as electronic messages or electronic documents, from unauthorised

access by the telecommunication service provider or any other third party, it is known to equally encrypt the data received by a user in such a manner that only those users may have access to the data for whom said data is intended. Both the encryption key and the decryption key may be stored in the above-mentioned secured environment. Thus the telecommunication service provider and any other third party are precluded from accessing either the traffic data or the user data. An unauthorised analysis of traffic data in the course of a grid investigation, for example, may thus be effectively prevented unless there is a warrant permitting the utilisation of the key deposited at a trusted party such as a notary public.

This method of securing traffic data and user data as known from the state of the art, however, has the disadvantage that even though the users of a telecommunication service are using secured communication connections to exchange data among each other, information on who is in communication with whom may still be derived from the data traffic by the telecommunication service provider. This information may be obtained by the telecommunication service provider even if the communication between the users and the telecommunication service is encrypted, as the contents of the data exchanged between the users is not needed for knowing who is in communication with whom.

This problem arises in particular in cases in which a telecommunication service, once it has received a message, such as an electronic document, from one user uses another message to signal to the user for whom the message is intended the presence of a message intended for him or her. Since the data exchange between the users and the telecommunication service is, as such, always "visible" for the telecommunication service provider, said telecommunication service provider, from the mere fact that a message for a particular user has been deposited by a user and that the user for whom the message is intended receives notice about the presence of the message, may receive the information that the two users are in communication with each other, even if the data exchange is carried out in an encrypted manner and the user for whom the message is intended does not request the latter from the telecommunication service.

Given the fact that the information on who is in communication with whom is part of the telecommunication traffic data which may be used in the course of a grid investigation or for creating personality profiles, the methods of preventive data retention as known from the state of the art are, despite high security standards, not sufficiently protected or secured to effectively preclude unauthorised data analysis.

US 2005/0076089 A1 discloses a method that is intended to make it possible for one or several senders to anonymously transmit messages to one or several recipients. The message transmitted by the sender is received by a third party that removes the sender information from the message which is then forwarded by said third party to the recipient. In order to make it more difficult to monitor message traffic, provision is made to store the received message at the third party for a given period of time and to forward it to the recipient only once this period of time has elapsed, together with other messages that may have arrived during this time period at the third party, all messages being forwarded in a single message and the sequence of the messages being randomly selected.

US 2006/0023727 A1 deals with a method of routing a message through a network which is intended to make sure that the sender of the message will remain anonymous. For this purpose, when the message is created, all information that might make it possible for one node within the network to identify the node at which the message was created is removed. Furthermore, a TTL field of the message, as it is called, is modified in order to prevent any node within the network from using the information contained in the TTL field to identify the node at which the message was created.

Object of the Invention

It is therefore an object of the present invention to provide a system and a method for securing telecommunication traffic data which, when at least one telecommunication service is used by a given number of users, is generated at the telecommunication service provider of said telecommunication service, which system and method effectively and efficiently prevent unauthorised access to, and abuse of, telecommunication traffic data.

Solution according to the Invention

This object is achieved, according to the invention, by a method and a system for securing telecommunication traffic data as claimed in the independent claims. Advantageous configurations and developments of the invention are stated in the respective dependent claims.

Provision is thus made for providing a method for securing telecommunication traffic data, which, when at least one telecommunication service is used by a given number of

users, is generated at the telecommunication service provider of said telecommunication service, the telecommunication service receiving a message of at least one first user of the telecommunication service which is intended for at least one second user of the telecommunication service, and the telecommunication service, in reaction to the reception of the message, sending a notification to the at least one second user, a predetermined time delay being provided between the reception of the message and the transmission of the notification, the time delay between the reception of the message and the transmission of the notification being selected depending on the data traffic volume per time unit between the users and the telecommunication service, the time delay being randomly selected from an interval of time delays and the interval limits of the time delay interval being selected depending on the data traffic volume per time unit between the users and the telecommunication service.

It is thus possible to preferably dynamically adapt the time delay or the transmission of the notifications to the work load of the telecommunication service.

In this manner it is possible to effectively prevent the current time delay from being determined using a time-based analysis of the incoming and outgoing data traffic, which might enable the telecommunication service provider, if he knows the current time delay, to establish a temporal correlation between the received messages and the transmitted notifications, from which the telecommunication service provider might derive information on who is in communication with whom.

The fact that the interval limits of the time delay interval are dependent on the data traffic volume per time unit between the users and the telecommunication service makes it possible to not only randomly select the time delay from the time delay interval but also adapt the time delay interval itself to the data traffic, such that it becomes still more difficult for the telecommunication service provider or for an unauthorised third party to determine the current time delay.
The time delay may be randomly selected from a time delay interval for a predetermined number of notifications to be transmitted. Alternatively, the time delay may be randomly selected from a time delay interval for each notification to be transmitted.

It has turned out to be particularly advantageous if the time delay is shorter at a high data traffic volume per time unit than at a low data traffic volume per time unit.

As in cases in which the data traffic volume per time unit is high, this typically means that messages from a great number of users are being received by the telecommunication service and, hence, notifications are transmitted to a great number of users, the time delay may be shortened without the telecommunication service provider having an opportunity to use a time-based correlation between the reception of the messages and the transmission of the notifications in order to derive information on who is in communication with whom. In cases in which the data traffic volume per time unit is low, the telecommunication service typically receives only messages from a small number of users and, therefore, needs to transmit a corresponding notification only to a small number of users. In order to make sure that even in such cases a time-based correlation between the reception of the messages and the transmission of the notifications may be precluded, the time-delay is augmented correspondingly.

It is advantageous if the telecommunication service is carried out in a secured environment (sealed infrastructure).

By carrying out the telecommunication service in a secured environment or sealed infrastructure, provision is made to make sure that the telecommunication service provider of the telecommunication service has no means of access to the data present at the telecommunication service. In order to also prevent any information to be derived from the data traffic between the users and the telecommunication service from which it might be derived who is in communication with whom, the time delay between the reception of a message and the transmission of the notification is provided. Thus, it may be avoided that by means of a time-based correlation between the reception of a message and the transmission of a notification it can be determined who is in communication with whom. Owing to the time delay, provision is made to avoid that a notification may be associated with a received message, such that also the sender of a message may not be associated with the recipient of the notification.

According to an advantageous configuration of the invention, the data traffic volume per time unit comprises the number of received messages per time unit. This is to avoid that in cases in which a small number of received messages per time unit which cause a great amount of data traffic due to the very big size of the messages, the time delay is selected too short, which, given the small number of received messages and transmitted notifications, might permit a time-based correlation between said received messages and said transmitted notifications.

According to one configuration of the invention, the telecommunication service may comprise a notification service which generates the notification to be sent to the at least one second user and triggers the time-delayed transmission of the generated notification, the time delay being determined by the notification service.

According to a configuration of the invention, the notification is transmitted to the at least one second user when said second user is logged in to the telecommunication service. Provision may also be made for not transmitting a notification to the second user when said second user is not logged in to the telecommunication service. Provision may be made for not transmitting a notification to the second user even though this second user has logged in to the telecommunication service Thus, an even better degree of decorrelation is achieved, i. e. associating of a notification to a received message may be made even more difficult.

The notification may comprise data adapted to output an acoustic and/or visual signal to the user indicating the presence of the message at the telecommunication service.

The notification may be identical from each user. According to one configuration of the invention, the notification may be transmitted in an unencrypted form. Since the notification is identical for each user, it may be transmitted in an unencrypted form, as no personal data whatsoever can be derived from the notification. The unencrypted transmission of the notification has the additional advantage that no encryption needs to be done on the part of the telecommunication service, which would mean an additional computing effort. The telecommunication service or the notification service which creates the notification and transmits it in a time-delayed manner may thus be carried out in a considerably more performing and resource-preserving manner.

According to one configuration of the invention, the message may be transmitted to the second user of the telecommunication service when requested by said second user. As the notification is sent in a time-delayed manner with respect to the reception of the message from the first user to the second user, it is not possible even from the request by the second user to transmit the message to the second user to derive any information on whether or not the first user is in communication with the second user.

The method according to the present invention has the advantage that the causality between the incoming messages and the notifications to be transmitted is abolished,

thus making it impossible to derive any information on who is in communication with whom.

The transmission of the message from the first user to the second user (via the telecommunication service) may be carried out on the basis of an end-to-end-encryption, i. e. the message is encrypted by the first user and is decrypted by the second user.

The message may be encrypted in a homomorphic manner.

In addition, the invention provides a system for securing telecommunication traffic data, which, when at least one telecommunication service is used by a given number of users, is present at the telecommunication service provider of said telecommunication service, the telecommunication service being adapted to receive a message which is intended for a second user from at least one first user and to transmit a notification to the at least one second user in reaction to the reception of the message, a predetermined time delay being provided between the reception of the message and the transmission of the notification, the telecommunication service being adapted to select the time delay between the reception of the message and the transmission of the notification depending on the data traffic volume per time unit between the users and the telecommunication service, to randomly select the time delay from an interval of time delays and to select the interval limits of the time delay interval depending on the data traffic volume per time unit between the users and the telecommunication service.

It has turned out to be advantageous for a system to comprise a secured environment in which the telecommunication service may be carried out.
The telecommunication service may comprise a notification service which is adapted to generate the notification to be sent to the at least one second user and to trigger the time-delayed transmission of the generated notification, the time delay being determined by the notification service.

In addition, the system of the present invention may further be adapted to carry out a method according to the present invention.

Brief Description of the Invention

Details and characteristics of the invention as well as specific example embodiments of the invention may be seen in the following description in conjunction with the drawing. In the drawings:

Fig. 1 is a system for securing telecommunication traffic data according to the present invention for explaining the inventive method of securing said telecommunication traffic data;

Fig. 2 shows the lapse of time between the reception of a message and the transmission of a notification; and

Fig. 3 shows two variants according to the invention for selecting a time delay depending on the data traffic.

Detailed Description of the Invention

The system of the present invention and the method of the present invention enable both, an adequate degree of data protection and sufficiently good possibilities for data evaluation, such as for investigative purposes. Abuse of the stored data, in particular the telecommunication traffic data, is effectively prevented, making it impossible, in particular, to derive any information from the data traffic on who is in communication with whom.

Fig. 1 shows a system according to the invention for securing telecommunication traffic data generated when a telecommunication service 10 is used by a given number of users T1 to Tn.
A telecommunication service provider 5 provides a telecommunication service 10 which is carried out in a secured environment U. The telecommunication service 10 may, for example, provide a message box where authorised users of the message box may deposit messages for other users. A message may, for example, be directly created in the message box or may be deposited in the message box via a communications network. A message may be, for example, an electronic document or the like.

In the example shown in Fig. 1, a message N, such as an electronic document, is transmitted by a first user T1 to the telecommunication service 10 and, for example, deposited there in a corresponding message box. Upon receipt of the message N, the

telecommunication service 10 creates a notification B within the secured environment and transmits it to the second user T2 via a communications network. The notification B informs the second user T2 about the fact that the first user T1 has deposited a message N for him in the message box of the telecommunication service 10.

According to one configuration of the invention, the telecommunication service 10 comprises a notification service 11 which is responsible for creating the notification to the second user T2 and for transmitting the notification.

Any data present at the telecommunication service provider 5, i. e. traffic data and user data, are stored and, if necessary, processed in the secured environment U. As explained at the beginning, both user data and traffic data may be stored in the secured environment U in an encrypted, preferably double encrypted, form. The double encryption makes sure that the telecommunication service provider 5 cannot have access to the user data and traffic data. The encryption or double encryption is preferably carried out within the secured environment U, with the keys necessary for this being created, stored, and managed in the secured environment U. The secured environment U is also referred to as a sealed infrastructure and prevents the provider of said infrastructure as well as the supplier of the telecommunication service or telecommunication service provider 5 from accessing this data during the data processing.

For this purpose, the secured environment U may comprise an apparatus, not shown in Fig. 1, for creating the required cryptographic keys. In order to prevent the communication data or user data which have been encrypted by the telecommunication service provider 5 in the secured environment U from being simply decrypted by the latter using the corresponding decryption keys, it is advantageous to encrypt the encrypted data for a second time using a further encryption key and to deposit the double encrypted data in a storage device of the secured environment U. The second encryption key may be handed over to a trusted party such as a notary public who may surrender it only by warrant of a court.

The secured environment U or sealed infrastructure may comprise a number of redundant and distributed computing resources which may respectively comprise a number of trusted platform modules (TPMs), as they are called, power switches for interrupting the energy supply of the entire computing resources, electromechanical

locks, a number of sensors by means of which the access to the computing resources may be monitored. According to one configuration of the invention, the computing resources may comprise storage devices in which the cryptographic keys are stored, with the cryptographic keys being stored, according to one configuration of the invention, exclusively on volatile storage media, such that an interruption of power supply will cause the stored keys to be deleted. Deleting the cryptographic keys may be necessary, for example, when someone has gained unauthorised access to a computing resource. In order to recover the keys, it is advantageous to synchronise the cryptographic keys via a synchronisation device that has a further storage device for storing cryptographic keys. The computing resources may be connected to a sealing control device, as it is called, which monitors the electromechanical components. If the sealing control device detects unauthorised access to a computing resource, it may cause the immediate synchronisation of all keys stored on said computing resource and, once the synchronisation has been completed, may interrupt the power supply to the compromised computing resource. It may thus be ensured that no further decryption keys can be created from a compromised computing resource.

The computing resources may further be coupled to a cloud control device, as it is called, which may be provided for carrying out the data exchange with one or several users T. The cloud control device may also be coupled to the sealing control device, such that the sealing control device may initiate protective measures even in cases in which an intrusion is detected to have taken place via a communications network.

The users T1 to Tn of the telecommunication service 10 may be smartphones, tablet PCs, conventional computers or the like, one user in the example shown in Fig. 1 being associated with one utilizer, respectively. As seen in Fig. 1 a data exchange is carried out between the users T1 and T2, and the telecommunication service 10, with data being transmitted from the first user T1 to the telecommunication service 10 and data being transmitted from the telecommunication service 10 to the second user T2, i. e. data from outside of the secured environment U being moved to the telecommunication service 10 or data from the telecommunication service 10 being moved out of the secured environment U and to a second user T2.

Even if the data exchange between the two users T1, T2 and the telecommunication service 10 is carried out in an encrypted manner, the telecommunication service provider 5 obtains information on the fact that the users T1 and T2 are engaged in a

(mutual) communication. In order to prevent the telecommunication service provider from obtaining the information, due to the data traffic, that the first user T1 is in communication with the second user T2 (without necessarily knowing the contents of the transmitted and/or received data), provision is made, according to the invention, that the notification B is created by the telecommunication service 10 or by the notification service 11 and transmitted to the second user T2 in a time-delayed manner. The time-delayed transmission of the notification B may ensure that the telecommunication service provider 5 cannot, from the data traffic, derive any kind of association between the received message N and the transmitted notification B, and that it is impossible for him to derive, from the traffic data, any information on the fact that user T1 is in communication with user T2. By providing a time delay between the reception of the message N and the transmission of the notification B, these traffic data, which are accessible from outside the secured environment U, are being "veiled", such that it is impossible for the telecommunication service provider 5 or for any other unauthorised third party to determine who is, how frequently, in communication with whom.

According to one configuration of the invention, the notification B may also be encrypted and transmitted in an encrypted form. This is advantageous, in particular, in cases in which the addressee of the message N is to be informed, via the notification B, about who has deposited the message N in a message box for him or about the kind of content of the message deposited in the message box.

However, it has turned out to be particularly advantageous for the transmission of the notification B to be accompanied solely by the information to the addressee or to the second user T2 that a message has been deposited for him at the telecommunication service provider 5. If the transmission of the notification B is accompanied only by the information that a message has been deposited, the notification B may be identical for all the users of the telecommunication service, such that an encryption, or encrypted transmission, of the notification B may be dispensed with. This may considerably reduce, or minimise, the workload of the system on the part of the telecommunication service provider while creating and transmitting the notifications.

According to one configuration of the invention it is sufficient if the user data of the notification B have a length of only one bit, as one bit is enough for the purpose of signalling to the second user T2 that some message has been deposited for him at the telecommunication service provider. Thus, the data volume necessary for the

transmission of the notifications B to the users of the telecommunication service may be reduced or minimised.

After having received the notification B, the second user T2 may request the message N intended for him from the telecommunication service provider. The communication between the first user T1 and the second user T2 may be carried out on the basis of an end-to-end-encryption, i. e. the first user encrypts the message and the second user decrypts the message N. A homomorphic encryption technique may be used to encrypt the message. This, for example, enables the telecommunication service to carry out operations on the message without having to decrypt the message itself. The result of the operation then is also present in an encrypted form.

Fig. 2 shows the timing of the reception of a message and of the transmission of a notification.

At time point t1, the telecommunication service of the telecommunication service provider receives a message from a first user. After having received the message, the telecommunication service or the notification service creates a notification for the user for whom the message is intended and transmits the notification to this user, with a predetermined time delay δt being provided between the reception of the message at time point t1 and the transmission of the notification. This is to say that the notification is transmitted to the second user at the time point $t1 + \delta t$.

In the simplest case of the invention, a constant time delay δt is used for all notifications to be transmitted. Such a constant time delay has the disadvantage, however, of being liable to be determined by means of an analysis of the data traffic between the users and the telecommunication service, such that once the time delay δt is known, an association of a notification B with a received message N may still be possible. In order to prevent this, provision may be made, according to the invention, to provide a dynamic time delay, which changes after a given number of notifications - at best after each notification. This makes it considerably more difficult, on the one hand, to determine a time delay by means of an analysis of the data traffic and, on the other hand, a determined time delay may be used solely for a few notifications transmitted in the past in order to correctly associate the notifications with their respective received messages, whereas a time delay determined in this manner would be worthless for an association

of notifications with messages for notifications transmitted, or messages received, in the future since the current time delay will already have change by that time.

Such a dynamics in the time delay δt may be achieved, for example, by selecting the time delay δt depending on the data traffic volume per time unit between the users and the telecommunication service.

Examples for the selection of a time delay δt depending on the data traffic volume per time unit are shown in Fig. 3.

In the examples shown in **Fig. 3**, the time delay at a high data traffic volume per time unit is shorter than that at a lower data traffic volume per time unit, i. e. that at a high data traffic the time delay δt may be selected to be shorter than that selected at a low data traffic, since a high data traffic will typically correspond to a great number of messages from a great number of users, such that an association of a transmitted notification with a received message will become more difficult by the mere presence of a huge number of transmitted notifications.

In the example shown in Fig. 3a, the time delay δt is not linearly dependent upon the data traffic, whereas in the example shown in Fig. 3b, the time delay δt is linearly dependent on the data traffic. It goes without saying that other dependencies between the time delay δt and the data traffic than those shown in Fig. 3a and Fig. 3b may be selected.

According to an configuration of the invention, the data traffic volume per time unit may comprise the number of received messages N per time unit. In order to achieve an even better dynamics of the selected time delay δt, provision may be made for the time delay δt required for the transmission of a notification to be randomly selected from a given time delay interval. In doing so, the time delay δt for a given number of notifications to be transmitted may be selected from said time delay interval. Alternatively, the time delay δt may be randomly selected from said time delay interval for each individual notification to be transmitted. It may thus be achieved that even if a comprehensive analysis of the data traffic between the users and the telecommunication service is carried out, no conclusions may be drawn concerning the association of the notifications with the received messages, as on the one hand each time delay is subject to a certain randomness and, on the other hand, due to the random selection of time delays for the notifications to be transmitted, the sequential order of the transmitted notifications will

no longer correspond to the sequential order in which the messages have been received.

The random component in the random selection of the time delay from a time delay interval may still be enhanced by selecting the interval limits of the time delay interval depending on the data traffic volume per time unit between the users and the telecommunication service. It may thus be ensured that at a high data traffic small time delays δt are being randomly selected from the time delay interval and at a low data traffic longer time delays δt are being selected from the time delay interval.

According to one configuration of the invention, provision may be made, in addition to alternatively to the above-mentioned measures for selecting a time delay, for the created notifications to be randomly ranked within a notification queue, such that the sequential order of the notifications to be transmitted will no longer correspond to the sequential order of the received messages When such a queue is used within which the notifications to be transmitted are randomly ranked, the random selection of a time delay from a time delay interval may be dispensed with, since it may be ensured by the random ranking of the notifications within the queue that even if a constant time delay is employed, it will not be possible for a transmitted notification to be correctly associated with a received message.

Reference Signs:

5	telecommunication service provider
10	telecommunication service
11	notification service
δt	time delay between reception of data and transmission of the notification
B	notification between telecommunication service and user
D	Data of the notification
N	message transmitted between user and telecommunication service
T	User
T1	First user
T2	Second user
U	Secured environment

PATENTKRAV

1. Fremgangsmåde til sikring af data i telekommunikationstrafik, som, når i det mindste én telekommunikationstjeneste (10) anvendes af et givent antal brugere (T), foreligger ved telekommunikationstjenesteudbyderen (5) for den nævnte telekommunikationstjeneste, hvor

- telekommunikationstjenesten modtager i det mindste én meddelelse (N) fra i det mindste én første bruger (T1) for telekommunikationstjenesten, som er bestemt til i det mindste en anden bruger (T2) for telekommunikationstjenesten, og
- telekommunikationstjenesten, som reaktion på modtagelsen af meddelelsen (N), genererer en notifikation (B) og sender denne til den i det mindste ene anden bruger, idet notifikationen (B) informerer den anden bruger (T2) om det faktum, at den første bruger (T1) har indleveret meddelelsen (N) til ham ved telekommunikationstjenesteudbyderen (5), idet en tidsforsinkelse (δt) er tilvejebragt imellem modtagelsen af hver meddelelse (N) og transmissionen af den tilsvarende notifikation (B), hvilken tidsforsinkelse (δt) mellem modtagelsen af meddelelsen (N) og transmissionen af notifikationen (B) er valgt afhængig af datatrafikvolumenet pr. tidsenhed imellem brugerne (T) og telekommunikationstjenesten,

kendetegnet ved, at

- tidsforsinkelsen (δt) er valgt tilfældigt fra et givet tidsforsinkelsesinterval, og
- intervalgrænserne for tidsforsinkelsesintervallet vælges afhængigt af datatrafikvolumenet pr. tidsenhed imellem brugerne (T) og telekommunikationstjenesten.

2. Fremgangsmåde ifølge krav 1, hvor tidsforsinkelsen (δt) er mindre ved et højt datatrafikvolumen pr. tidsenhed end ved et lavt datatrafikvolumen pr. tidsenhed.

3. Fremgangsmåde ifølge ethvert af de foregående krav, hvor tidsforsinkelsen (δt) vælges til at være forskellig for et forudbestemt antal notifikationer eller for hver notifikation.

4. Fremgangsmåde ifølge ethvert af de foregående krav, hvor datatrafikvolumenet pr. tidsenhed omfatter antallet af modtagne meddelelser (N) pr. tidsenhed.

5. Fremgangsmåde ifølge ethvert af de foregående krav, hvor telekommunikationstjenesten (10) omfatter en notifikationstjeneste (11), som genererer notifikationen (B),

som skal sendes til den i det mindste ene anden bruger (T2) og trigger den tidsforsinkede transmission af den genererede notifikation, hvilken tidsforsinkelse (δt) bestemmes af notifikationstjenesten og telekommunikationstjenesten eksekveres i et sikret miljø (U).

6. Fremgangsmåde ifølge ethvert af de foregående krav, hvor notifikationen (B) omfatter data (D) indrettede til at afgive et akustisk og/eller visuelt signal til den anden bruger (T2), som indikerer tilstedeværelsen af meddelelsen (N).

7. Fremgangsmåde ifølge ethvert af de foregående krav, hvor notifikationen (B) er identisk for hver bruger (T).

8. Fremgangsmåde ifølge ethvert af de foregående krav, hvor notifikationen (B) transmitteres på en ikke-krypteret måde.

9. Fremgangsmåde ifølge ethvert af de foregående krav, hvor meddelelsen (N) transmitteres til den anden bruger af telekommunikationstjenesten (10), når det anmodes af den anden bruger (T2).

10. Fremgangsmåde ifølge ethvert af de foregående krav, hvor transmissionen af meddelelsen (N) fra den første bruger (T1) til den anden bruger (T2) udføres på basis af en ende-til-ende-kryptering, idet meddelelsen fortrinsvis er krypteret på en homomorf måde.

11. System til sikring af data i telekommunikationstrafik, som, når i det mindste én telekommunikationstjeneste (10) anvendes af et givet antal brugere (T), foreligger ved telekommunikationstjenesteudbyderen (5) for telekommunikationstjenesten, hvilken telekommunikationstjeneste er indrettet til at modtage en meddelelse (N), bestemt til en anden bruger (T2), fra i det mindste én første bruger (T1), og som reaktion på modtagelsen af meddelelsen (N), at generere en notifikation (B) og sende denne til den i det mindste ene anden bruger, hvilken notifikation (B) informerer den anden bruger (T2) om det faktum, at den første bruger (T1) har indleveret meddelelsen (N) til ham ved telekommunikationstjenesteudbyderen (5), idet en forudbestemt tidsforsinkelse (δt) er tilvejebragt imellem modtagelsen af meddelelsen (N) og transmissionen af notifikationen (B), idet telekommunikationstjenesten er indrettet til at vælge tidsforsinkelsen (δt)

mellem modtagelsen af meddelelsen (N) og transmissionen af notifikationen (B) afhængigt af datatrafikvolumenet pr. tidsenhed imellem brugerne (T) og telekommunikationstjenesten,

kendetegnet ved, at

telekommunikationstjenesten yderligere er indrettet til

- at vælge tidsforsinkelsen (δt) tilfældigt fra et givet forsinkelsesinterval, og
- at vælge intervalgrænserne for tidsforsinkelsesintervallet afhængigt af datatrafikvolumenet pr. tidsenhed imellem brugerne (T) og telekommunikationstjenesten.

12. System ifølge det foregående krav, hvor telekommunikationstjenesten (10) omfatter en notifikationstjeneste (11), som er indrettet til at generere notifikationen (B) til at blive sendt til den i det mindste ene anden bruger (T2), og at trigge den tidsforsinkede transmission af den genererede notifikation, idet tidsforsinkelsen (δt) er bestemt af notifikationstjenesten og systemet omfatter et sikret miljø, i hvilket telekommunikationstjenesten kan eksekveres.

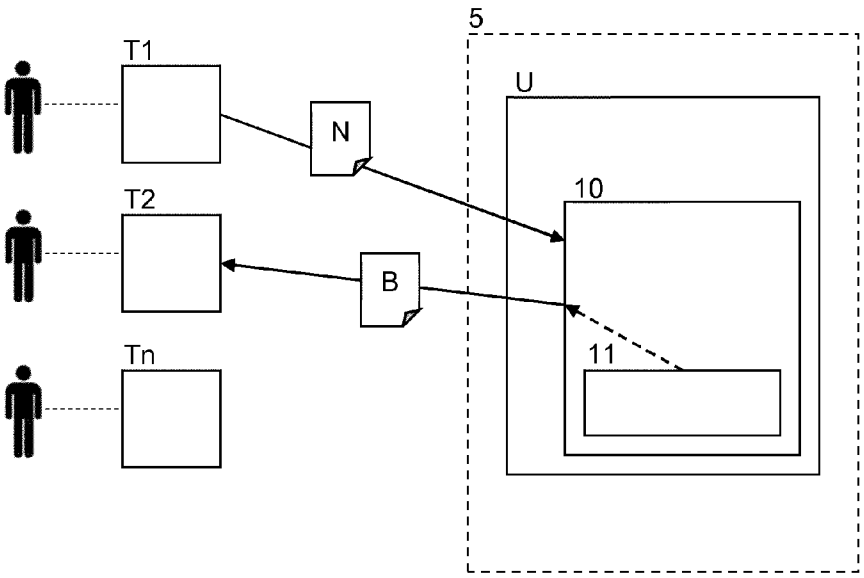

Fig. 1

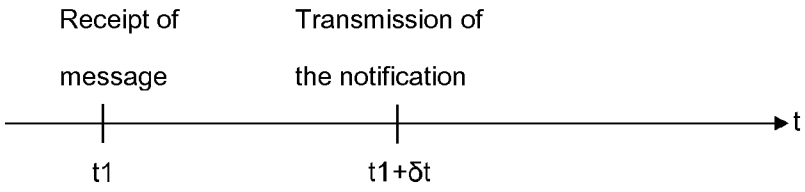
Receipt of
message
Transmission of
the notification
t
t1
t1+δt

Fig. 2

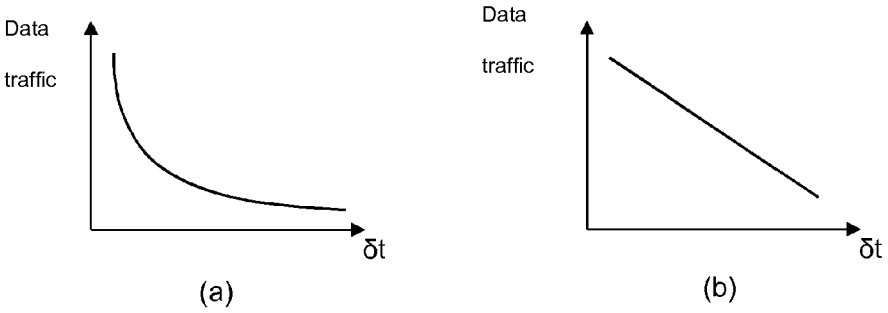
Data
traffic
δt
(a)
Data
traffic
δt
(b)

Fig. 3