

(19) **DANMARK**



Patent- og
Varemærkestyrelsen

(12)

Oversættelse af europæisk patentskrift

(10) **DK/EP 3568964 T3**

-
- (51) Int.Cl.: **H 04 L 9/40 (2022.01)** **H 04 L 9/08 (2006.01)** **H 04 L 9/32 (2006.01)**
H 04 L 51/04 (2022.01) **H 04 L 67/12 (2022.01)** **H 04 W 4/14 (2009.01)**
H 04 W 12/033 (2021.01) **H 04 W 12/041 (2021.01)**
- (45) Oversættelsen bekendtgjort den: **2023-09-04**
- (80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2023-06-28**
- (86) Europæisk ansøgning nr.: **17832313.5**
- (86) Europæisk indleveringsdag: **2017-12-29**
- (87) Den europæiske ansøgnings publiceringsdag: **2019-11-20**
- (86) International ansøgning nr.: **FR2017053867**
- (87) Internationalt publikationsnr.: **WO2018130761**
- (30) Prioritet: **2017-01-10 FR 1750212**
- (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: **Wallix, 250 Bis Rue du Faubourg Saint-Honoré, 75008 Paris, Frankrig**
- (72) Opfinder: **BINSZTOK, Henri, 7 rue Boutarel, 75004 Paris, Frankrig**
- (74) Fuldmægtig i Danmark: **Novagraaf Brevets, Bâtiment O2, 2 rue Sarah Bernhardt CS90017, F-92665 Asnières-sur-Seine cedex, Frankrig**
- (54) Benævnelse: **FREMGANGSMÅDE TIL ENDE-TIL-ENDE-OVERFØRSEL AF EN KRYPTERET DIGITAL INFORMATION OG SYSTEM TIL IMPLEMENTERING AF FREMGANGSMÅDEN**
- (56) Fremdragne publikationer:
EP-A1- 1 788 770
EP-A1- 2 680 207
WO-A1-2016/195590
AU-A1- 2013 205 071
US-A1- 2002 129 238
Alan Henry: "The Best Cloud Storage Services that Protect Your Privacy", , 7 octobre 2010 (2010-10-07), pages 1-13, XP055409356, Extrait de l'Internet: URL:https://lifel hacker.com/the-best-cloud- storage-services-that-protect-your-priv-7 29639300 [extrait le 2017-09-22]

METHOD FOR END-TO-END TRANSMISSION OF A PIECE OF ENCRYPTED DIGITAL INFORMATION AND SYSTEM IMPLEMENTING THIS METHOD

Description

Field of the invention

- 5 The present invention relates to the field of securing asynchronous electronic communication on computer networks, in particular, but not limited to the Internet or virtual private networks.

The information, such as digital data produced by connected objects, faxes, or text messages, digital files, are transmitted by means of a standardized set of data
10 transfer protocols, which makes it possible to produce varied applications and services such as the publication of data, email, instant messaging, peer-to-peer, etc.

The most secure solutions use end-to-end encryption techniques. When a message is sent to a recipient, it is encrypted by the user, on the computer
15 equipment of the transmitter, according to solutions guaranteeing that only the receiver can decrypt the correspondence. The server through which the conversation passes is only used as relay, without ever attempting to decode it. In this case, users can communicate with one another without intermediaries.

Instead of being sent in text form, the message is scrambled in a numerical format
20 and a key is required to decrypt it. The keys are ephemeral and disappear when the message has been decrypted by the user. Because of this, pirates, cybercriminals and even service operator employees are not able to read the correspondence. By way of example, the messaging service WhatsApp (trade name) offers an end-to-end encryption solution.

25 State of the art

Patent application WO2014175830 discloses a method for processing a data packet from a first computing device to a second computing device in order to allow end-to-end encryption communication.

The data packet comprises an encrypted message using a first encryption key in order to form an encrypted message, data for identifying the second computing device encrypted using a second encryption key in order to form encrypted identification data, and first and second encrypted encryption keys.

- 5 The method according to this known solution consists in decrypting the encrypted second encryption key, decrypting the encrypted identification data using the decrypted second encryption key, and transmitting the data packet according to the decrypted identification data, the encrypted message and the first encryption key being designed not to be decrypted by the server to allow end-to-end
10 encryption communication between the first and second computing devices.

Patent application WO2012067847 also describes systems and methods for end-to-end encryption. In accordance with one embodiment, a device registration method comprises the following steps:

- an application executed by a computer processor receives a user password
15 from a user;
- by means of the computer processor, the application combines the user password and an extension of the password;
- by means of the computer processor, the application cryptographically processes the combination of the user password and the extension of the
20 password, which makes it possible to obtain public cryptographic information. The public cryptographic information is provided to a server. However, the user password is not provided to the server.

Also known is patent EP1536601, which relates to an end-to-end encryption method of email sent from a transmitter to a recipient comprising the following
25 steps:

- a) the transmitter asks an encryption system for a certificate corresponding to said recipient,

b) the encryption system returns to said transmitter a first certificate corresponding to said recipient, the transmitter sends with his email software an outbound email to said recipient. encrypted with said certificate,

c) said email is sent by said encryption system.

- 5 The encryption system decrypts the email using a private key corresponding to the certificate, and the encryption system makes the content of said email available to said recipient.

The transmitter requests a certificate corresponding to said recipient from an encryption system in said private network, the encryption system returns to said
10 transmitter a first proforma certificate corresponding to said recipient, the proforma certificate being generated or recovered by the encryption system for the recipient and only used between the transmitter (1) and the encryption system, the transmitter sends with its email client an outbound email to said recipient encrypted with said proforma certificate, said email is transmitted via said
15 encryption system, said encryption system decrypts said email by using a private key corresponding to said certificate, and said encryption system makes the content of said email available to said recipient.

In the prior art, U.S. patent US7240366 describes an end-to-end authentication method based on the public key certificates combined with the Session Initiation
20 Protocol (SIP) to allow a SIP node that receives a SIP request message to authenticate the sender of the request. The SIP request message is sent with a digital signature generated with a private key of the sender and may include a certificate of the sender. The SIP request message can also be encrypted with a public key of the recipient. After receiving the SIP request, the SIP receiver node
25 obtains a certificate from the sender and authenticates the sender based on the digital signature.

The digital signature can be included in a header for authorizing the SIP request or in a message body in several parts constructed in accordance with the standard S/MIME.

Patent application US20100189260 describes a solution for managing rights assigned to a communication session and to the components related to the user's request. The participants authorized to participate in the session are provided with access tools such as decryption keys. Restrictions based on the assigned
5 conversation rights are extended to preserve the records and associated documents of the communication session.

Drawbacks of the prior art

The solutions of the prior art allow end-to-end transmissions of data or encrypted messages only between a transmitter previously registered on a transactional
10 platform and a recipient, also previously registered on a transactional platform.

When a transmitter wishes to send a message or data to a recipient that is not already registered, he must first send him a non-encrypted message inviting him to register on the transactional platform.

During this time, the transmitter must keep the message in memory of his
15 computer equipment, monitor the receipt of a notification of registration of the recipient, and then undertake the process of transmitting the message or encrypted end-to-end data with the newly registered recipient.

The interception of the invitation message sent by the transmitter can be intercepted, thus opening a security breach.

20 Moreover, if a long delay elapses between the sending of the invitation and the notification of the registration of the transmitter, the message or the data may be lost or altered.

In any case, the solutions of the prior art require synchronization mechanisms between the computer equipment of the transmitter, that of the recipient and the
25 transactional platform.

In particular, in the solution proposed by patent application US20100189260 (Figure 3), users are already known to the platform, which does not allow communication with a recipient not known to the platform.

The solutions of the prior art also have a security defect known by the name of man-in-the-middle attack, which is an attack that has the purpose of intercepting communications between two parties, with neither one aware that the communication channel between them has been compromised.

5 Solution provided by the invention

The invention is defined by the independent claims. Particular embodiments are defined in the dependent claims.

Detailed description of a non-limiting example of the invention

10 The present invention will be better understood from reading the following description, which refers to one non-limiting exemplary embodiment shown by the appended drawings, in which

- Figure 1 shows a schematic view of the hardware architecture of a system for the implementation of the invention
- Figure 2 shows a diagram of data exchanges between Alice and Bob
- 15 - Figure 3 shows a block diagram of the step of temporarily registering Alice's message
- Figure 4 shows the diagram of generating information from the password chosen by Bob
- Figure 5 shows a block diagram of the step of re-encrypting the message by
20 Alice
- Figure 6 shows a block diagram of the step of retrieving the message by Bob

Hardware architecture

25 Figure 1 shows a schematic view of the hardware architecture, in a simplified situation concerning exchanges just between two users.

The users are called Alice and Bob, and each use one or more items of connected computer equipment, respectively (1, 11; 2, 12). It may for example be a connected computer or a tablet, or a smartphone.

When it is a computer, it is necessary for it to have computing resources to access
5 a network, for example the Internet, and a standard web browser.

In the case of a tablet or a telephone, the equipment also comprises resources such as a browser or a mobile application ensuring connection to a remote platform.

The system according to the invention optionally implements a proxy (3), which
10 distributes the load of the service to one or more servers (4, 13, 14) that can be local or remote in the “cloud”, executing an interactive programming interface (API).

The servers (4, 13, 14) are associated with one or more items of database management equipment (5, 15, 16), which may be local or remote in the “cloud”.

15 The communication between the various devices uses a standard transport layer, for example TCP/IP or Lora, and a standard communication layer, for example http or https.

The proxy (3) and the servers (4, 13, 14) as well as the database management equipment (5, 15, 16) form a secure exchange platform (20).

20 Diagram of exchanges

The initiator of exchanges is Alice, wishing to transmit to Bob a message in a secure form via a platform, it being understood that Bob does not have access to the exchange platform (20).

Alice composes locally, on one of her devices (1, 11), a digital message (21) with
25 any editor, for example a messaging application suitable for the platform (20), and therefore client of the APIs (4, 13, 14) and records locally in buffer memory one of her devices (1,11).

Alice then inputs a public identifier (22) of the recipient Bob, for example Bob's messaging address or a mobile telephone number, in the application executed on her equipment (1, 11).

This application then controls the opening of a communication session with its identifier. The application then controls the sending of a request via the platform (20) for the transport layer and via this session and, for the communication layer, via the session token (or equivalent mechanism), for identifying Bob, in the form of a message comprising at least Bob's identifier.

The platform (20) compares the identifier (22) transmitted by Alice with the list of identifiers of the holders of an account by a verification step (23).

If Bob is unknown, that is to say does not have an account on the platform (20), the platform generates a temporary account associated with Bob's identifier transmitted by Alice.

This temporary account results in:

- 15 - creating an entry dedicated to Bob in the database (5, 15, 16)
- sending by the platform (20) a message to Bob containing:
- a text message (25) from Bob's information that there is a message coming from Alice
- a link to a creation interface (26) for Bob to create a password, for example
- 20 in the form of JavaScript and HTML code.

This creation interface (26) is executed immediately or later on Bob's equipment (2), locally and without communicating the string of characters (27) created by Bob to the platform (20) or to the Alice's equipment (1, 11) and more generally to any equipment present on the network.

25 The platform (20) then transmits to Alice an acknowledgment message. Sending this message means that:

- the platform (20) has created a temporary account assigned to Bob

- the platform (20) has transmitted to Bob the message (25) containing the link allowing him, whenever he wishes, to proceed with the step of entering a password in the interface (26).

Temporary Recording of Alice's message

- 5 Figure 3 shows a block diagram of the step of temporarily registering Alice's message.

The receipt of the message automatically triggers the following operations:

- Alice's client application controls the encryption of the message (21) with Alice's public key (19), transmitted by the platform (20) from the information
10 recorded in the database (5, 15, 16) and corresponding to her account. This public key is for example transmitted in the message or in the process of opening the session. It can also be stored locally on Alice's equipment (1, 11), for example in the cache memory of a mobile application. This step leads to an encrypted message (42) containing generally non-encrypted metadata, in particular an
15 identifier of the recipient Bob.
- this encrypted message (42) is then transmitted by a transmission (102) to the platform (20) and recorded, for example:
 - in the database (5, 15, 16) of the platform (20)
 - in a third-party mailbox linked to Alice
 - 20 - in a platform in the Cloud...

The platform also records in the database (5, 15, 16) of the platform (20) the metadata (43) containing in particular the message storage address, for example in the form of a URL address.

- 25 Optionally, Alice's equipment (1, 11) generates a random encryption key (44) enabling the symmetric encryption of the message (42). This random key (44) itself is encrypted asymmetrically with Alice's public key (19) so as then to allow Alice to decrypt the random key (44) with her own private key.

Generating Bob's public and private information

This step is asynchronous relative to the exchange process. It occurs at any time after the receipt of the notification of the message (25) and of the associated link.

Figure 4 shows the detail of the procedure for creating Bob's public and private
5 information.

The password (27) can be entered by Bob on a physical or virtual keyboard. It can also be generated by a code generator type equipment.

This password (27) undergoes processing by the creation interface (26) to generate:

- 10 - a hash (28) by applying a known cryptographic algorithm
- optionally one or more random numbers (29)
- a pair of public (30) and private (31) keys.

From the code executed from the creation interface (26), Bob creates a character string (27) constituting a password.

- 15 In the example, the creation interface (26) generates a random number (29).

The creation interface (26) controls the calculation of three digital sequences:

- an optional hash (28), by applying a Sha512 type processing, for example, to the character string (27), after optionally applying a salting algorithm to this string (27)
- 20 - a pair of public / private keys, respectively (30, 31), by applying a processing, such as PBKDF2, to a combination of the random number (29) and the password (27).

The result of these operations leads to:

- secret data that will not be transmitted by Bob to third parties: it involves the
25 password (27) and the private key (31)

- public data, that are transmitted to the platform (20) and recorded in Bob's account: the hash (28), the random number (29) and the public key (30).

Re-encrypting the message by Alice

When Alice has transmitted to the platform (20) the encrypted message (42) as mentioned with reference to Figure 3, and Bob has, asynchronously, proceeded to enter a password as mentioned with reference to Figure 4, the conditions for finalizing the exchange between Alice, already having an account, and Bob, who did not have an account at the time the message (21) was sent, are satisfied.

Figure 5 shows a block diagram of the step of re-encrypting the message by Alice.

10 In an automatic execution mode, when one of Alice's equipment (1, 11) is connected to the platform (20), the platform (20) controls a step of re-encrypting (52) the message (42) on one of Alice's equipment (1, 11), and not on the platform (20).

15 If necessary, for example when the equipment (1, 11) does not have a cache, this operation provides the transmission (103) by the platform (20) to Alice's connected equipment (1, 11) of:

- Bob's public key (30)
- the metadata (43) associated with the encrypted message (42)
- optionally the encrypted message (42) on Alice's connected equipment .

20 First alternative

According to a first alternative, the platform (20) transmits to Alice the entirety of the encrypted message (42), and Alice decrypts this message with her private key, then re-encrypts it with Bob's public key (30) that the platform has just sent to her (20).

25 The original message (21), initially encrypted with Alice's public key (19) in order to produce a transient encrypted message (42), is now available in a new form (45) encrypted with Bob's public key.

The message (42) is deleted from the platform (20) and replaced by the encrypted message (45).

This variant requires heavy processing for large messages.

Second alternative

- 5 According to another alternative, the platform (20) sends to Alice only the random key (44). Alice decrypts this random key (44) with her private key, then re-encrypts the random key (44) thus decrypted with Bob's public key (30) that the platform (20) has just sent to her.

- 10 In this case, the encrypted message (42) is kept, only the associated metadata (43) are updated on the platform via an automatic request from Alice.

This variant makes it possible to simplify the processing of a large volume message.

Retrieving the message by Bob

Figure 6 shows a block diagram of the step of retrieving the message by Bob.

- 15 After this re-encryption operation, the platform (20) sends Bob a digital message comprising a text or automatic notification enabling him to retrieve the encrypted message from Alice.

- 20 Alternatively, Bob's application periodically queries the platform (20) to determine the availability of new messages, or else Bob connects manually to the platform (20) to determine whether new messages are available.

During the connection, Bob's computing equipment (2, 12) executes a processing similar to the one shown in Figure 5, from the password (27) that he initially had created, and the random number (29) initially recorded on the platform (20).

- 25 This allows Bob to regenerate the public key (30) and the private key (31), which is never stored and is never sent over the network.

Bob can then retrieve the encrypted metadata (43) and on the other hand the encrypted message (42 or 45, depending on the variant), and carry out their decryption with his private key (31).

- For subsequent exchanges, both parties have an account on the platform (20)
- 5 enabling them to communicate in an end-to-end encrypted mode.

Functional Architecture of a connected object

In the case where the exchanges are not between two persons having computer equipment, but between connected objects or a connected object and a person, the connected object has an architecture of which Figure 6 shows an example.

- 10 The connected object comprises in a known manner a computer (300) associated with a network communication circuit (301).

- It comprises a non-volatile memory area (302) in which at least one digital sequence corresponding to the password (27) is recorded. Optionally, the non-volatile memory (302) may also contain a second digital sequence corresponding
- 15 to the random number (29).

PATENTKRAV

1. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital information mellem en afsender, der er registreret på en transaktionsplatform (20), og mindst én modtager, hvilken fremgangsmåde omfatter følgende trin:

- 5 • valg, på afsenderens computerudstyr (1, 11), af en digital information og en digital identifikator for modtageren,
- temporær kryptering af den digitale information ved afvikling af en lokal krypteringsapplikation på afsenderens computerudstyr (1, 11) med en nøgle for afsenderen,
- 10 • overførsel, med afsenderens computerudstyr, af den krypterede digitale information og identifikatoren for modtageren til transaktionsplatformen (20),
- overførsel, ved hjælp af transaktionsplatformen (20), til modtagerens computerudstyr (2, 12)
 - af en digital invitationsbesked, der omfatter et link, hvis aktivering foretaget
- 15 af modtageren iværksætter følgende:
 - afvikling af en applikation til generering, på modtagerens computerudstyr (2, 12), af mindst ét par krypteringsnøgler for modtageren
 - overførsel af mindst én offentlig nøgle for modtageren, der således genereres af modtagerens computerudstyr (2, 12), til transaktionsplatformen (20)
- 20 og registrering deraf på platformen i forhold til identifikatoren for modtageren,
- overførsel til modtagerens computerudstyr, med afsenderens computerudstyr (1, 11), af den digitale information, der er krypteret med modtagerens offentlige nøgle, eventuelt via transaktionsplatformen (20),
- dekryptering, med modtagerens computerudstyr, af informationen med
- 25 modtagerens private nøgle, hvor afsenderens nøgle er afsenderens offentlige nøgle, og **ved at** fremgangsmåden yderligere, efter registrering af den mindst ene offentlige nøgle og inden trinnet til overførsel, til modtagerens computerudstyr, af

den digitale information, der er krypteret med modtagerens offentlige nøgle, omfatter følgende trin:

- notificering, ved hjælp af transaktionsplatformen (20) til afsenderens computerudstyr (1, 11), af en digital besked, der muliggør hentning og lagring, i en
5 temporær hukommelse på afsenderens computerudstyr, af modtagerens offentlige nøgle samt digital information, der er krypteret med afsenderens nøgle,
- dekryptering, på afsenderens computerudstyr (1, 11), af den digitale information, der er krypteret med afsenderens nøgle, derefter kryptering af den digitale information med modtagerens offentlige nøgle, en fremgangsmåde, hvor
10 generering af det mindst ene par krypteringsnøgler omfatter et kryptografisk processeringstrin, der anvendes for en kombination dannet af et kodeord, der vælges af modtageren, og et engangskodeord, der overføres af modtageren, og et engangskodeord, der ved hjælp af transaktionsplatformen overføres til modtagerens computerudstyr, idet fremgangsmåden, når den anvendes for en
15 gruppe, der udgøres af en flerhed af modtagere, omfatter følgende:
 - et trin til indføring af unikke intermediære krypteringsnøgler for hver digital information,
 - idet hver modtager får adgang til den digitale information ved dekryptering af de intermediære nøgler med de personlige nøgler,
 - 20 • trin til genberegning af intermediære nøgler i tilfælde af, at gruppen af adressater modificeres.

2. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital information ifølge krav 1, hvor krypteringsapplikationen består af en WEB-applikation, der af computerplatformen overføres til afsenderens computerudstyr i
25 form af kildekode, der kan afvikles af en browser med JavaScript.

3. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital information ifølge krav 1, hvor krypteringsapplikationen består af en mobilapplikation, der tidligere er installeret på afsenderens computerudstyr.

4. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital information ifølge krav 1, hvor mindst én krypteringsapplikation udgøres af en mobilapplikation, der kan downloades, til installation deraf på modtagerens computerudstyr, og **ved at** den digitale invitationsbesked indeholder en mekanisme til iværksættelse af downloadingen.
5. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital information ifølge krav 1, anvendt for en gruppe digitale informationer, hvilken fremgangsmåde omfatter:
- et trin til indføring af unikke intermediære krypteringsnøgler for hver digital information,
 - idet hver modtager får adgang til sættet af gruppen af digitale informationer ved dekryptering af de intermediære nøgler med de personlige nøgler.
6. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital information ifølge krav 1, hvor mindst ét element af computerudstyret udgøres af en tilsluttet genstand.
7. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital information ifølge krav 6, hvor genereringen af krypteringsnøglerne omfatter et kryptografisk processeringstrin, der anvendes for en kombination dannet af en unik hemmelig information, der er registreret i den tilsluttede genstand på tidspunktet for fremstillingen deraf, og et engangskodeord, der overføres ved hjælp af transaktionsplatformen.
8. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital information ifølge krav 1 til en beskedtjeneste.
9. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital information ifølge krav 1 til en fildelingstjeneste.
10. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital information ifølge krav 1 til en real-time-multimediekommunikationstjeneste.

11. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital information ifølge krav 1 til en digital informationskommunikationstjeneste med en tilsluttet genstand.

12. Fremgangsmåde til overførsel af en ende-til-ende-krypteret digital
5 information ifølge krav 1 til en digital informationskommunikationstjeneste med en tilsluttet medicinsk indretning.

13. System, der omfatter en tilsluttet genstand, hvilket system omfatter en unik og hemmelig information, der er registreret på tidspunktet for fremstillingen deraf, en processor til afvikling af applikationer, der er registreret i en lokal hukommelse,
10 og midler til kommunikation med en transaktionsplatform, **kendetegnet ved, at** én af de registrerede applikationer er i stand til at afvikle de processeringskørsler på modtagerens computerudstyr, der er specifikke for fremgangsmåden ifølge krav 1, idet det mindst ene par af modtagerens krypteringsnøgler genereres ud fra den unikke og hemmelige information, idet systemet yderligere omfatter
15 transaktionsplatformen og et computerudstyr hos en afsender til implementering af fremgangsmåden ifølge krav 1.

14. System ifølge det foregående krav, hvor den tilsluttede genstand yderligere omfatter en regnemaskine (300), der er forbundet med et netværkskommunikationskredsløb (301), og et ikke-flygtigt hukommelsesområde
20 (302), hvor der registreres mindst én digital sekvens svarende til kodeordet (27).

Figure 1

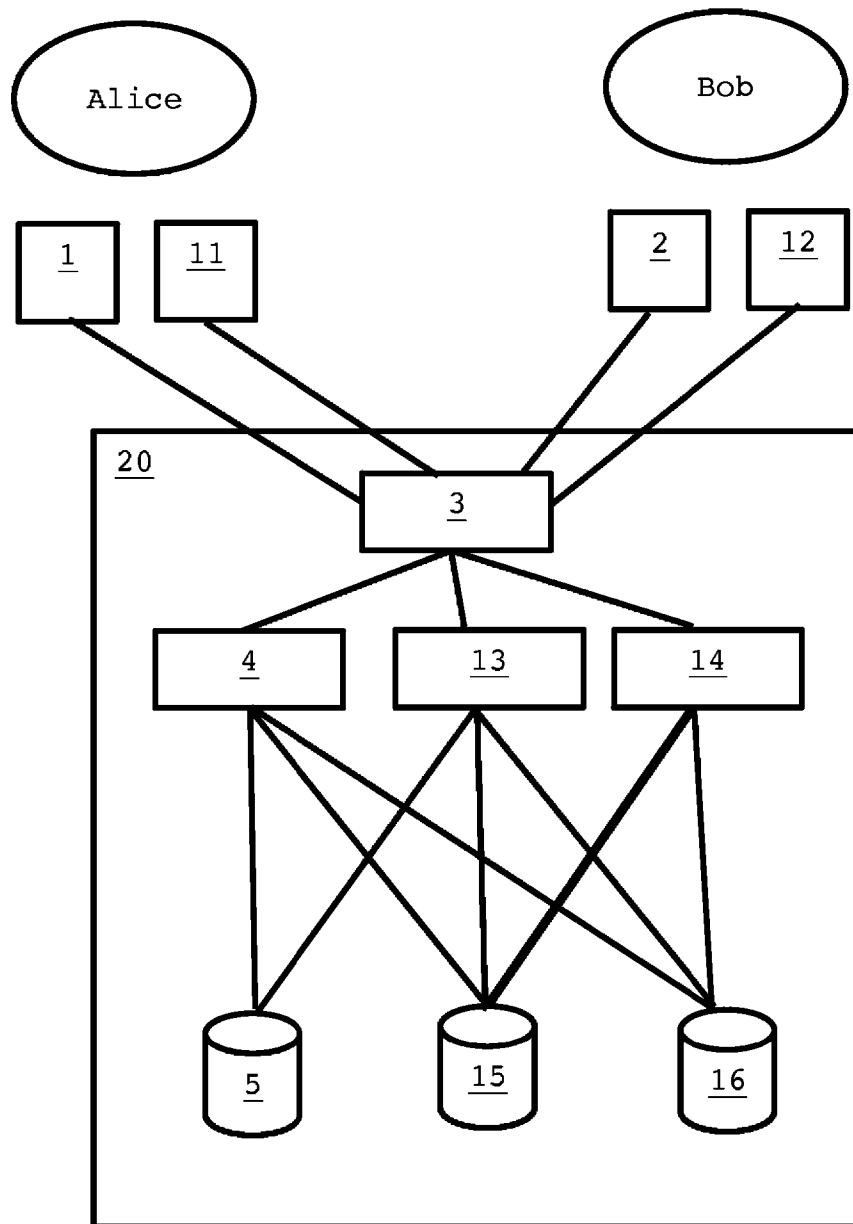
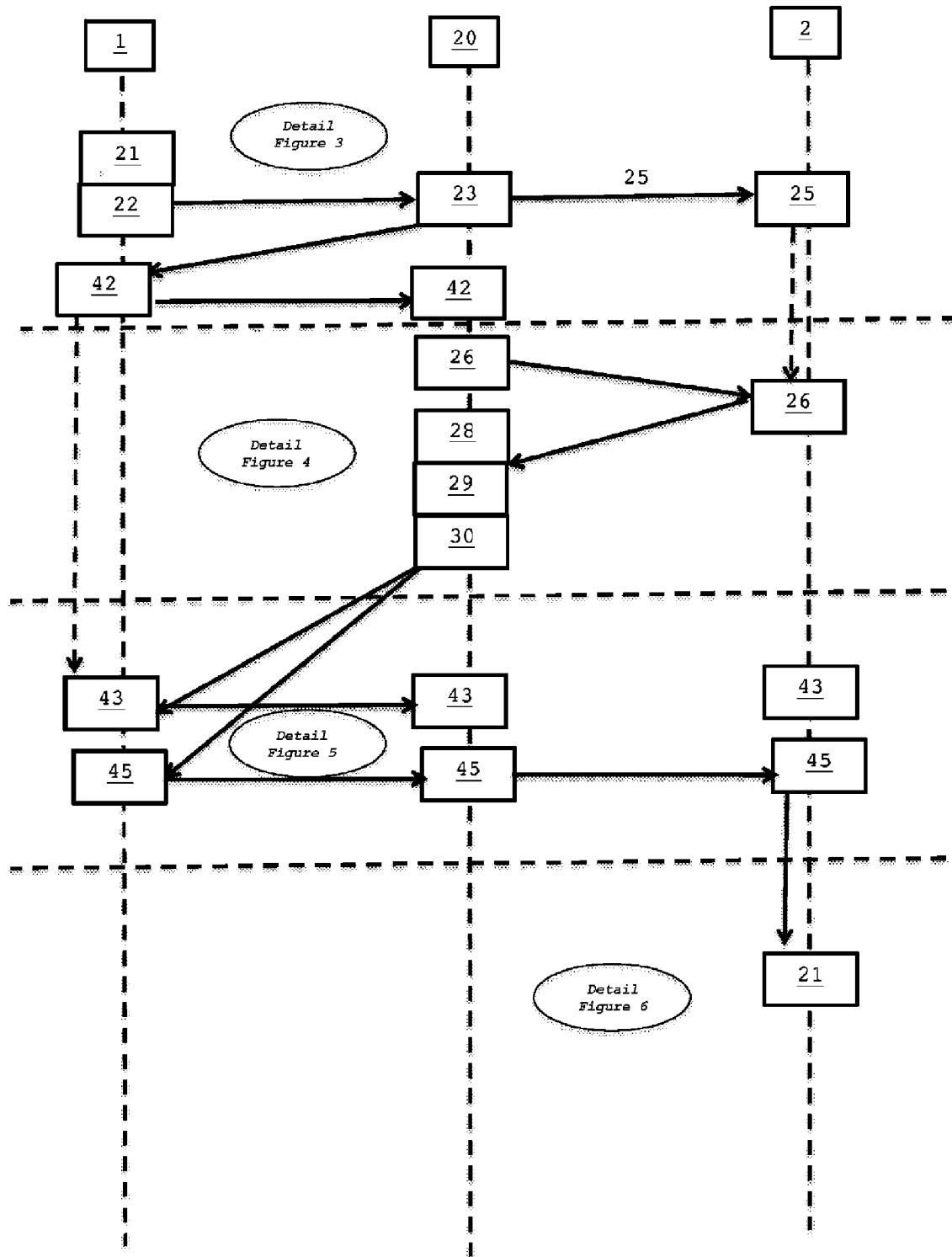


Figure 2



3 / 4

Fig. 3

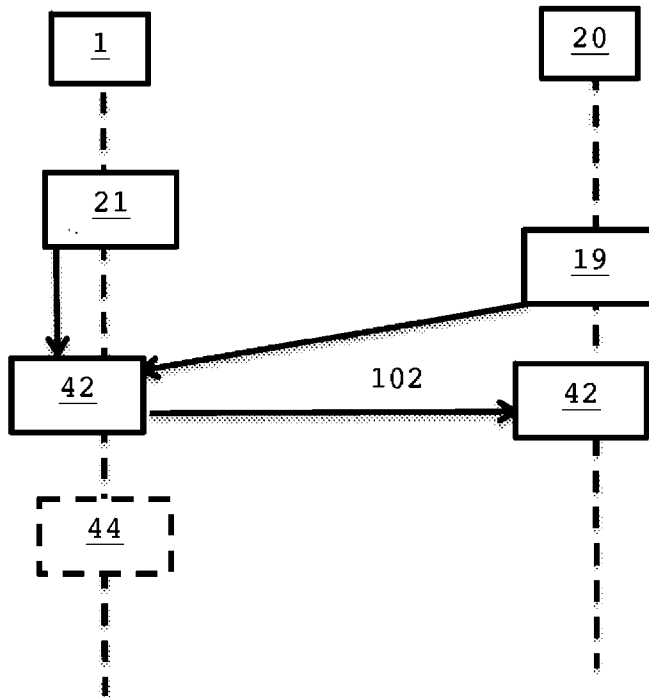
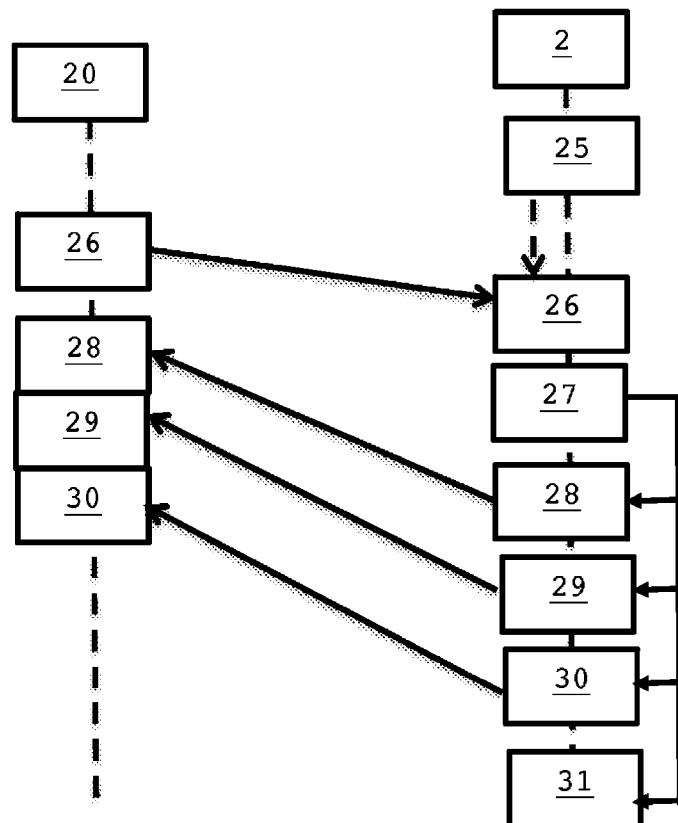


Fig. 4



4 / 4

Fig. 5

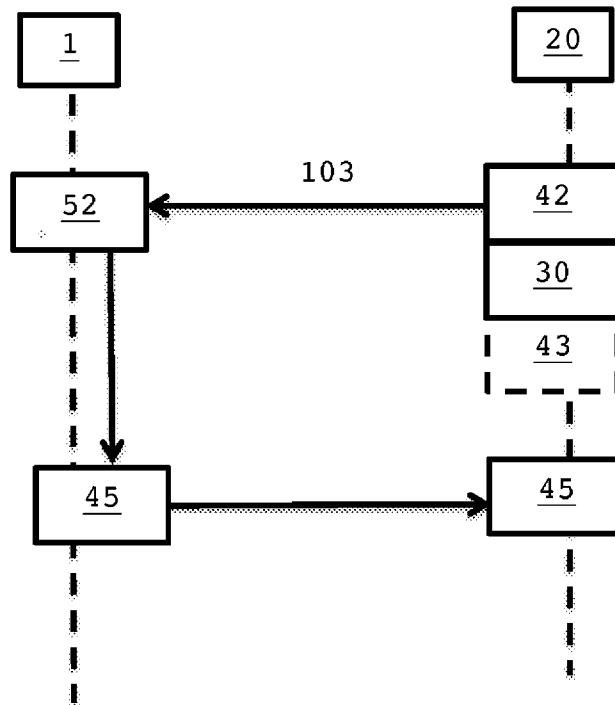


Fig. 6

