Notice

DESCRIPTION EP2575298B1

10 The invention relates to an encryption method for messages that are sent from a transmitter to a receiver within a LAN (Local Area Network) and / or a WAN (Wide Area Network), further a device for a secure information channel for communication between a transmitter and a Receiver, a method for encrypting data that is transmitted between a first and second communication terminal and further a method for encrypting data that is between a computer (Mac, PC, client / server, handheld but also smartphone) and a data carrier or a data source released in a network.

1.

20 Encryption of emails

21 E-mails can be encrypted, for example, by means of client-based e-mail encryption or server-based e-mail encryption.

23 Client-based e-mail encryption has the disadvantage that it involves a greater effort for the end user and is difficult to manage for a layperson without prior technical knowledge. The end user must first request a certificate ("public key") from the recipient for encryption, then encrypt and send the e-mail with it. He must manage the certificates, keep them up to date and properly secure them. If he wants to receive an email, he must provide a certificate ("public key"), receive the email and open it with his own certificate ("private key"). With his own certificates, he must also take care of proper storage, updating and securing. If the end user acts in a company network and the certificates are not managed or stored centrally, there is a considerable administrative overhead because each client in a network takes over its own certificate management.

33 Server-based email encryption systems also help here. However, these have the disadvantage that they are too complex and expensive for many organizations and especially for private end users. A suitable IT infrastructure is required for a server-based e-mail encryption system, which is administered administratively. The work for the administration of the certificates is taken over from each individual user, the work is centralized and systematized, but is not unnecessary. An

administrator with access to all the necessary information also represents a risk factor.

39 Both systems have the disadvantage that certificates have to be administratively administered, saved, secured and updated. Furthermore, encryption is not carried out without a certain amount of work. If third parties seize the systems, they can manipulate the user to damage them.

43 According to EP 1536601, an encryption system is therefore proposed which already encrypts emails within the sender's own company network. In order to make e-mails secure within a system, an e-mail server sends so-called pro forma certificates to the clients, which use them to encrypt the e-mails. A disadvantage of the system is the high level of technical complexity and also the risk that the server or client can be manipulated.

48 EP 1788770 also describes a method of secure e-mail communication between the sender and recipient, the sender encrypting the e-mail with a public key of the recipient, which is already present in the own database or is still being queried from the recipient sent. As described in FIG. 2 of EP 1788700, the encryption system consists of software and hardware components with an operating system such as "Windows Server" or "Linux", which are operated on a server in a computer domain. However, this hardware deployment is expensive and since the computer components have a MAC or IP address, the encryption system can also be controlled and manipulated.

56 Furthermore, US 2008/0282078 A1 describes a dedicated mail gateway that encrypts received user data ("plain text mail") and forwards it to a recipient, the essential function being to determine an error in the transmission and encryption process and to send the user this information to inform. This server-side encryption solution has the disadvantage of an installation and administration effort and can also be manipulated due to the available addresses.

62 US 2007/0192583 describes a bridge which is transparently integrated between a LAN and a WAN and whose task is to protect a (home) computer from dangers from the Internet. However, the proposed device does not have the functions of autonomous encryption and key management provided according to the present invention.

2.

69 Encryption of files and data carriers

70 In addition to the data that is exchanged via a network (LAN or WAN) (emails, chat, etc.) and only temporarily stored on volatile memories, there is also the need to access data that is stored indefinitely before access To protect third parties. It makes no difference whether the data is on a tangible data medium such as a USB stick, an internal / external hard drive or the like or on a network drive (local network) or no longer on the local computer or in the company data center, but in a (metaphorical) cloud, called "cloud". In any case, it may be necessary to transmit data securely, that is to say encrypted, and then to store them in encrypted form on the storage elements and to make them accessible only by authentication with a certificate.

78 According to the state of the art, some programs are available on the market. BitLocker is, for example, hard disk encryption from Microsoft ®, which is included in the Ultimate and Enterprise

versions of the Windows Vista ® and Windows 7 ® operating systems and in Windows Server 2008 ® and which, as an alternative or in addition, allows you to enter a PIN with a key file (available via USB stick) to start the system or request files.

83 TrueCrypt ® (www.truecrypt.org) is also a software for data encryption, in particular it is used for the complete or partial encryption of hard disks and removable media.

85 TrueCrypt ® knows three ways of working with encrypted data: An entire device (for example a hard disk) or an existing partition is encrypted. Existing data can be received and encrypted here before encryption. So-called container files can also be created. Containers are particularly suitable for creating a private encrypted area for sensitive data on an otherwise unencrypted partition. However, the user must mount the file to read and write, the user must always have a certificate and a good password for proper encryption. Both systems have in common that they involve considerable effort for the end user and that they must be familiar with the secure handling and storage of certificates and passwords as well as with the use of encrypted areas. Because often no readable headers are created for the encrypted files and also a file structure (e.g.

95 (NTFS or FAT) is not preserved, amateurish or careless handling can quickly lead to the irretrievable loss of all data.

97 The task of the present connection is to provide a system with a device that can be connected to a computer (Mac, PC, client / server, handheld but also smartphone), connects it to a network infrastructure and the task of key management, the Encryption and decryption takes over fully automatically and can encrypt both e-mails or general user data as well as files and thus transmit them securely in a network and / or store them securely on a data carrier. The device must be integrated into a system so that it cannot be controlled and manipulated by unauthorized third parties.

104 The solution to the problem results from claims 1 and 14, advantageous embodiments can be found in the subclaims.

106 Description of the invention In one embodiment, the device has interfaces such as. B. Ethernet, WiFi, Bluetooth or cellular interfaces or the like, via which it integrates a computer into a LAN or WAN. Intended use of the device should not only be suitable for a computer, i.e. a home PC or a company PC (client, server), but also for a Mac, a handheld, a smartphone, a tablet PC or a gateway, in the case of a handheld, a smartphone, a tablet PC or a gateway, the device can be designed as an embedded system.

112 The device is a technical link that does not have its own MAC or IP address and is therefore invisible to third parties and other devices in the network infrastructure. The device cannot be controlled directly. On the other hand, by reading a data stream between a transmitter and a receiver (supervised computer), the device knows the MAC or IP address of the computer it supervises. If this address changes, it carries out a reset according to the invention and initializes and restructures itself when the device is connected to a new computer. Furthermore, the user can of course also carry out a hardware reset and thus initiate the initialization and restructuring.

120 With the help of an identification program, an encryption program and a key management program, the necessary steps are carried out in order to send securely encrypted messages or

general user data from a transmitter to a receiver within a LAN and / or a WAN, a secure information channel for communication between a transmitter and to set up a receiver or to transmit encrypted files in a generally secure manner between a first and a second communication terminal. The device works completely autonomously and without administrative intervention, the programs run as a routine.

127 The

128 Identification program

129 reads a data stream between a transmitter and receiver.

130 It identifies the communication protocol and determines the application level, further identifies the user data and filters it out.

132 The user data and the identification features of the user data are passed on to the encryption program.

134 The encryption program requests that the identification characteristics of the user data be passed on to the

136 Key management program

137 from this one appropriate and necessary for encryption.

138 After a plausibility check as to whether the relevant key is available, the user data is encrypted. The encryption program, because files are regularly larger than 1518 bytes (Ethernet protocol) and files are broken up as file fragments and transmitted in various ways, the file fragments in one processes logical order, whereby early arriving file fragments are temporarily stored and processed when they are due and a previous encrypted usage date is included in an associated later usage date during encryption.

144 According to the invention, the file fragments are not put together, but processed as file fragments and forwarded immediately.

146 The data stream is only adjusted to the extent that an original chronology is restored; since the "flow" is encrypted like in a "synchronous translation", communication takes place in real time, since the duration of an operation (including a waiting time) is predictable.

149 Task of

150 Encryption program

151 is the reverse of decryption in addition to encryption.

152 When decrypting, a private key that corresponds to the public key received is decrypted.

153 If an incorrect or outdated public key was used on the transmitter side, there are four options:

154 the program sends an error message because it could not decrypt the usage date

155 the program sends the message back because the usage date could not be decrypted

156 the program is not already accepting the message because the identification features of the user date indicate an outdated or incorrect key

158 the message is forwarded to the recipient unencrypted.

159 The encryption program is preferably able to proceed according to the third option because, due to the identification features provided by the identification program, it is able to recognize an error early on and initiate encryption and to avoid further work steps.

162 The

163 Key management program

is able to comprehensively manage your own private, your own public and third-party public keys, make them available to the encryption program or an external third party (sender), generate your own keys and ensure their timeliness based on plausibility criteria.

It is able to generate a key application-specific and protocol-specific and, if required, user-specific.

This means that the key for various applications, such as for e-mail messages, for chat communication, for storing information on a homepage or platform or in a social network, is generated, kept available and made available .

The key also corresponds to the respective requirements of the communication protocols.

As already mentioned, the key can also be made for a particular user (sender by e-mail sender, visitor to a website, etc.).

The key management program accordingly manages an extensive and multi-level database.

The key management program maintains the implemented database and keeps keys, i.e. your own as well as the foreign keys, up to date.

In this way, your own keys are renewed according to a logic.

Reasons for an update can be:

Compromise of the key

Timing

abusive multiple queries from third parties

Connection of the device to a new computer (new identity)

Hardware reset by user

Foreign (public) keys are requested:

first time sending messages to recipients

Compromise of a saved key

Timing

if a message has not arrived at the recipient and has to be sent again

Connection of the device to a new computer (new identity)

Hardware reset by user

If there is no foreign public key (sending a message to the recipient for the first time), this is queried from the recipient by sending a message addressed to the recipient (or his computer) to the recipient.

Because the device does not have an address, a message cannot be sent directly to the device.

Because the device's identification program is reading the data stream, it will identify the message and forward it to the key management program for response.

The autonomously working key management program will answer the key query and send the key back to the sender with a message.

Preferably, the identification or key management program, after reading and processing the key query message, will delete it so as not to burden the recipient with unnecessary information.

A key query can itself be encrypted.

The messages are addressed to the respective computer of the sender or recipient, but these are "intercepted" by the devices and answered.

206 The computers are not burdened with any message traffic.

207 Because an email also remains with the sender until the recipient creates a data stream and the recipient's device then reads the data stream and answers the key query of the sender's device, the email traffic is further reduced.

210 The recipient creates a data stream, for example, by switching on his computer and querying his mailbox.

212 For fast communication, it is conceivable to regularly query external keys from recipients after a certain period of time, which is particularly useful when there is intensive communication.

214 However, the key management program preferably queries public keys from recipients if the recipients are in an internal list X, had received a number of Z messages in the period Y and preferably the number of messages is in a high ratio in relation to the total messages sent; this ratio is particularly preferably 0.8.

218 A new key is also requested when the recipient's device sends an error message or when a sent message comes back.

220 For security reasons, foreign keys are always deleted when the device is connected to a computer with its own identity with the new identity.

222 Furthermore, all keys are deleted when the device is opened.

223 The described, autonomously working programs interlock, the tasks are not strictly assigned to one program, but can also be carried out by another program.

225 Other programs implemented on the device are also designed in such a way that intervention from "outside", that is to say from third parties, is not possible.

227 They run completely autonomously without administrative access.

228 In a further embodiment according to the invention, the device has an additional addressable module which has identification features such as an IP address or MAC address and which also independently processes and answers tasks according to the inventive concept.

231 The addressable module manages information that requires user (computer) or administrator (network) intervention.

233 The addressable module itself can also take over functions of a router.

234 The addressable module also enables you to manage whitelists and blacklists, to use virus scanners or to apply user management.

236 User management means managing a database in which users (third parties) are noted, who are granted certain rights and who have their own key to exercise their rights, the rights to decrypting user files such as texts, Images, music related to applications such as Facebook, Xing or other blogs.

240 The addressable module then creates further user-specific metadata for each user (third parties), which supplement the identification features of the useful files that are stored in the applications mentioned.

243 1. Example of message transmission by email

244 a. Send an email

245 If a user sends an email according to the state of the art, he will encrypt it himself or send it to a dedicated email server, which carries out the encryption and forwards the email to the recipient.

248 If an e-mail is received by a dedicated e-mail server, it is regularly available in one package and in the application layer.

250 Since no fragmented files go through no application layers and processing does not have to be carried out in real time, encryption or decryption can be done without time pressure and "organizational" sorting effort.

253 According to the prior art, there are also keys in an administered database, which the server simply has to access for decryption or encryption.

255 However, the method according to the invention is to run autonomously without administrative help, in real time if possible, file fragments being sorted and buffered under the greatest time pressure, and at the same time the recipient's public key required for encryption is to be queried by a key management program.

259 According to the invention, this task is solved as follows:

260 According to the invention, the user sends an email in "plain text" to the recipient.

261 According to the invention, the identification program implemented in the device reads the data stream between the transmitter and the receiver.

263 It identifies the communication protocol and determines the application level, further identifies the user data and filters it out.

265 The user data and the identification features of the user data are then passed on to the encryption programs.

267 By forwarding the identification features of the user data to the key management program, the encryption program requests the relevant public key of the recipient.

269 Because files are regularly larger than 1518 bytes (Ethernet protocol) and files are fragmented as file fragments and transmitted in various ways, the encryption program will process file fragments in chronological order; File fragments arriving prematurely are temporarily stored and processed when they are due, with a previous encrypted usage date being included in an associated later usage date during encryption.

274 According to the invention, the file fragments are not put together, but processed as file fragments and forwarded immediately.

276 The data stream is only adjusted to the extent that an original chronology is restored.

277 The data stream is passed through in real time like a synchronous translation.

278 The key management program mentioned uses the identification features transmitted by the identification program in an internal database to check whether the recipient and his "public key" are already known.

281 Identification features can accordingly be name, alias name, e-mail address, MAC or IP address or the like.

283 These identification features are stored in the internal key database and a public key of a recipient is assigned to them.

285 At the same time, the key management program performs an automatic plausibility check, e.g.

286 B. with regard to timeliness of the public recipient key by.

287 As part of the plausibility check, features such as age, authenticity, hash value and compatibility with the encryption system are checked.

289 If the plausibility check is negative, a new public key is immediately requested from the

recipient.

The following applies:

1.

If the public key is available in your own database, the e-mail with the public key is encrypted and sent by the encryption program.

The recipient's device will check the received email as described above, then decrypt it with its own private key and make it available to the user.

The basic setting of the device is that all emails are always encrypted.

Encryption of emails can only be dispensed with in exceptional cases if this is noted in a so-called whitelist.

Such a whitelist can be created in an internal database and implemented in the addressable module.

The user can access the database on the addressable module via a user interface and has the option of individualizing, supplementing or improving it.

The same applies to an already mentioned list of unwanted transmitters ("spammers"), a so-called "blacklist", which is also via an encrypted connection (TLS or

SSL) is queried.

In both cases, the device authorizes itself using the addresses (MAC or IP) of the computer it manages.

2.

If the public key is not available in your own database, the key management program will send a request to the recipient, presenting your own public key.

The submission of your own public key is used for identification.

If the recipient also has the device according to claim 1, this will automatically answer the request and transmit a public key to the sender's device, which the sender's key management program automatically takes over into its own management.

The sender's device will then encrypt the email as described in step 1 and send it to the recipient.

On the part of the recipient, in turn, the device becomes active according to the invention, reads the data stream, recognizes the e-mail on the basis of the file structure and carries out the steps as under "b.

Receiving an email "as described.

3.

If the other party (recipient) does not have a device and should still send an email to it, the following options are available:

a. The device sends a request to the opposite side and requests the public key of the addressee on presentation of its own public key and receives it directly or as an attachment to an e-mail and carries out the further steps as described in section 1.

b. The device converts the email into a password-protected PDF and sends it, or the device creates a container and inserts the file to be encrypted there.

332 For security reasons, a second channel is selected for sending the password, so the opposite side can receive a password by SMS, FAX or telephone, the device being used for the purpose of password transmission of the addresses of the "supervised" computer or according to a further embodiment of the Address of the "addressable module" operated.

336 SMS are sent via a signaling channel of the GSM standard such as SDCCH (Stand-alone Dedicated Control Channel) or FACCH (Fast Associated Control Channel).

338 However, the device does not establish a connection itself, but causes either the "supervised" computer or the addressable module.

340 The same can be done with the password transmission by fax, here the addressable module can either send an e-mail to a gateway, which then forwards it as a fax (Mail2Fax) or the device uses the service of an authorized and trustworthy service provider.

343 c. The recipient of the email is listed in one of the aforementioned whitelists and receives an unencrypted email.

345 d. The email is not delivered and remains in the user's outbox.

346 Basically, the original e-mail always remains in the computer's outbox until one of the options a) to c) has been carried out.

348 If the email is not sent, the user receives an error message.

349 According to the preference that all e-mails are always sent encrypted, the user receives a report when an e-mail has been sent unencrypted (according to the requirements of the whitelist).

352 Since the communication between the device and the computer takes place directly and not via the public network, the risk that information can be manipulated is minimized or reduced by the user, who always maintains the computer properly, regularly installs updates, one Set up firewall and run a virus scanner.

356 Another starting point to improve the security of public keys is to provide the keys with an expiry date.

358 However, the user cannot - and this should be expressly emphasized - access the device itself because the device has no addresses.

360 It is therefore not possible to configure the device in any way.

361 In order to give the user a choice between different options, one uses a protected and configurable, already mentioned addressable module.

363 b. Receive an email

364 1.

365 First of all, it was used in the context of email communication.

366 The identification program implemented in the device recognizes an email and its sender.

367 Optionally, it compares their senders with an internally maintained spam list ("spammer"); if the comparison is positive, the e-mail is sorted out, stored in a quarantine container and finally deleted in a (repeat) case confirmed by the user.

370 According to the invention, these functions are to be carried out by a scanner program located on the addressable module.

372 Accordingly, the spam mail is deleted immediately after a stricter regulation, because "communication" between the user and the device to exclude manipulative interventions is not

desired.

375 The comparison will therefore take place via an external spam list ("spammer"), which is queried by a trustworthy and authorized service provider.

377 Processing can also take place via the administrative module.

378 2.

379 The file checked after step 1 is then checked for malware (viruses, worms, Trojans).

380 If the result is disadvantageous here, the file is also placed in a quarantine container.

381 Because the security of e-mail traffic is paramount and communication between the user and the device is undesirable, the file is preferably not forwarded here, but deleted immediately.

383 As a rule, the user will not be interested in receiving emails or user data that contain malware.

384 3.

385 After positive completion of the optional security checks in accordance with numbers 1 and 2, a complex decryption procedure runs in mirror image to the encryption procedure, whereby a private key is used for decryption.

388 If the sender (third party) used an incorrect, compromised key or outdated key, the following options arise because decryption cannot be carried out:

390 the encryption program sends an error message to the recipient

391 the encryption program sends a message to the sender (third party)

392 the encryption program does not accept the email and deletes it

393 the encryption program passes the encrypted email on to the supervised computer

394 the encryption program sends the email back

395 The encryption program preferably sends the email back because the sender (third party) will then recognize the error and have the option of sending the email a second time.

397 If the sender (third party) has the device according to the invention, it will request a new, current public key from the recipient during the encryption process due to the internal logic according to which the key management program operates and carry out the encryption procedure with the recipient.

401 2. Example: Connection of data carriers

402 In a further embodiment already described, the device has an addressable module which has further looped-through interfaces such as USB, FireWire, Thunderbolt or the like in addition to Ethernet or radio interfaces such as WLAN or Bluetooth.

405 As already mentioned, the device is integrated into a network via Ethernet, be it WLAN / LAN or WAN, so that network drives can also be "connected" via this.

407 The network drives are addressed and integrated by the computer or addressable module; the addresslessly integrated device only reads the data stream.

409 The same applies to the other connections, such as the USB connection, so that the device only reads the data that flows between the computer and the USB device.

411 The addressable module automatically mounts corresponding external data carriers.

412 Similar to the encryption of an e-mail, the device also takes over the further complete processing of encryption or

414 Decryption, starting with the identification of user data, which is carried out with the help of a key provided by the key management program via the encryption or

416 Decryption performed by the encryption program.
417 Here, too, the appropriate key is assigned to each use, for example to query a file, to open a partition or an entire drive.
419 If access to the corresponding data source becomes possible, it can be called up and decrypted "on the fly".
421 When writing, encryption is also done "on the fly".
422 In addition to this, the data release can be made more secure by using a PIN, a password or other security features.
424 A program required for this is installed on the addressable module.
425 The integration of technical solutions such as identification via RFID chip is just as possible as with NFC (Near Field Communication).
427 The main advantage for the user is that they do not have to deal with the technical requirements that are running in the background and, in contrast to the state of the art, do not have to spend any time and thought for secure encryption.
430 Except for the possible entry of a PIN, the user will not notice anything because the device processes the processes autonomously in the background.
432 This represents a considerable time and labor saving for the user.
433 As part of cloud computing, files in the cloud, i.e. are stored on a file system in an IT infrastructure of a third party and the rest of the procedure is carried out in the same way so that files are stored in encrypted form, protected against access by third parties.
436 Encryption is possible with all methods that are common in the state of the art, such as S / Mime or PGP. The encryption programs are preinstalled regularly or can be installed as part of a program upgrade.
439 Since the device is not addressable, this is left to a specialist.
440 According to the invention, the device encrypts the transmitted data, the file and folder structure as well as the file system (NTFS, FAT) remaining unencrypted.
442 Here, too, the goal is to encrypt the security-relevant, so-called useful data, which the device recognizes on the basis of the file structure, usually on the basis of the header.
444 Compared to the prior art, this offers the major advantage that non-encrypted files can also be inserted into the existing folders in the existing file system.
446 Another advantage is that files, whether encrypted or unencrypted, can be copied without any problems.
448 Another significant advantage over the prior art, as described above, is that when a data carrier is mounted, it is recognized by the operating system and not, as is the case with a data carrier that is encrypted with TrueCrypt, remains unrecognized and is irrevocable due to a system prompt from the user and complete deletion caused by negligent handling.
452 3. Example: encryption of a chat
453 There is also a need for encrypted transmission of chat communication via the Internet.
454 If two users are chatting over the Internet, the page structure of the website is maintained regularly and this is only supplemented by the communicative text on the respective user interface.
457 Therefore, there is a regular need to encrypt this additionally by a text added by the user.

458 The device is able to recognize and encrypt this text based on the file structure.
459 The device operates similarly to the methods of email or file encryption described above.
460 If there is a device on both sides, the exchange runs without problems as follows, without the user even noticing:
462 The identification program reads the data stream, analyzes the communication protocol, determines the application level, identifies the user data and forwards the identification features to the encryption program which, upon presentation of the same, asks the key management program for a key.
466 If a public key of the recipient is not available, the latter will request the recipient's public key by presenting his own public key and will receive it from the recipient's device.
468 The user file is then encrypted using the public key and transmitted to the recipient.
469 This decrypts the text using the device and its own private key so that it is included in "plain text".
471 When responding in chat, communication is handled in the opposite way.
472 This ensures that the chat is encrypted over the Internet and is only transmitted between the device and computer in unencrypted form and finally on the display of the sender's computer or
475 The recipient appears in plain text.

4.

479 Example: Setting up a VPN tunnel
480 Likewise, if the device according to claim 1 is present on both sides, a VPN tunneling can be established.
482 VPN tunneling to an external device to be integrated is established using VPN software that is available on the device.
484 Depending on the VPN protocol used, the network packets can also be encrypted within this VPN tunneling.
486 With the help of this method known from the prior art, a connection can thereby be made bug-proof and tamper-proof, even if a connection to the VPN partner is established through an insecure network.
489 Authentication of the VPN endpoints can be guaranteed by using passwords, public keys or a digital certificate.
491 According to the invention, the exchange of the public keys is carried out autonomously.
492 In addition, the device also performs the encryption as in 1. 1. and 1.b, with the data being sent to the recipient in encrypted form using the recipient's public key.
494 The reverse is the case.
495 The recipient device encrypts using the requested transmitter key.
496 Here, too, the user does not have to worry about exchanging certificates.
497 Since the device does not have any addresses (MAC, IP), it uses - as already mentioned - the addresses of the "supervised" computer or preferably the addressable module and uses them to set up and process communication.

5.

503 Example: Encrypted information on homepages or in social networks

504 A user who wants to save or store information for third parties such as images, texts or sounds and encrypt them on a homepage or a social platform, for example, selects the "Encryption of user data" option via a program (add-on on browser).

507 Then, for example, a web interface gives him the option to choose at least the following options:

509 Name of the user data to be encrypted (image, text, sound)

510 Duration of the provision of the data

511 Naming of the users (third parties) to whom the data are accessible (user-specific)

512 After the input of the data has been completed, the identification program or the encryption program is activated, and the user data or the identification data of the user data are supplemented by so-called metadata.

515 According to section 1.a, encryption then takes place.

516 A visitor who accesses the page and has a device is made aware of the encrypted file and asked if he would like to read it.

518 The detailed procedure is as follows:

519 The identification program reads the data stream and recognizes the identification features of the user data and the other metadata.

521 It then forwards the identification data and the metadata to the encryption program.

522 The encryption program uses this data to query the key program for the associated key.

523 If a key is available in the key management program, it passes the key on to the encryption program for decrypting the user data.

525 If a key is not available, the user is queried according to the scheme already described, in contrast to the scheme described in section 1, further information is requested or requested from the computer being serviced or preferably from the addressable module (user-specific data) whether the user is authorized to obtain the key.

529 If he is authorized, the user's key management program sends the key to the supervisor's computer.

531 The upstream device reads the data stream, recognizes the information and uses it to decrypt the data as already described in Section 1. b.

533 If the user is not authorized, they simply do not receive the key.

534 It is therefore advisable to have the addressed module, which also offers router functions, in permanent operation.

536 On this addressed module, as already described, the data is stored, which user data may be accessed by which user within which time period.

538 The entire process takes place very promptly, so that we can speak of real-time transmission (soft real time),

540 According to the invention, a system is therefore proposed, consisting of at least two devices according to the invention, each of which is assigned an addressable module in order to

ensure smooth and fast communication or a smooth and fast data exchange.

543 Figure description

544 The invention is illustrated schematically in FIGS. 1 and 2 below.

545 In Figure 1, two laptops can be seen on the top left representing the senders, and two receivers on the bottom right.

547 The sent e-mails pass through stations 1 and 2 and are sent over the Internet, symbolized by the globe, to stations 3 and 4 and then to two recipients.

549 The stations 1-4 have the following meaning:

550 1.

551 User usually sends an email.

552 Special settings or even a configuration or additional software are not necessary.

553 2. The device (safeN @ il) filters the email out of the line, takes care of the exchange of the necessary keys with the recipient and encrypts the message before it leaves the local network.

555 3.

556 At the recipient, the email is filtered out of the data flow again and - before it is passed on to the local network - decrypted by the device (safeN @ il) with the appropriate certificate.

558 Spam is recognized and filtered here.

559 4.

560 The recipient of the message receives the email without additional effort.

561 Like the sender, he is not dependent on any software.

562 Manual intervention is not necessary.

563 Figure 2 shows the exchange of the "public key".

564 The device used in the process is also referred to here as "SafeN @".

565 With the lock symbol, as in FIG. 1, the encryption or

566 Symbolizes decryption ("encrypted transfer").

567 When sending an e-mail, the device automatically generates a key request.

568 On the recipient side, the device answers and transmits the recipient's public key.

569 With this key ("public key") the e-mail to be transmitted can be encrypted and transmitted securely - only the recipient can decrypt the message with his private key ("private key").

571 When the message arrives, it is filtered out of the data flow again, decrypted and passed on to the recipient in the local network.

573 The key exchange is carried out autonomously - without user intervention.

574 As already shown in detail, the device designated here as "safeN @", which is used in the method according to the invention, is an autonomous device which is transparently integrated into the LAN and which filters emails out of the data flow of the line , interpreted and corresponding processes or

578 Communication processes and routines start or work through.

579 The user himself has neither configuration nor installation effort, while he is not bound to certain manufacturers or brands in terms of software or hardware.