

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017565 A1

(51) International Patent Classification⁷: **H04L 9/00**

(21) International Application Number: PCT/BY01/00012

(22) International Filing Date: 20 August 2001 (20.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant and

(72) Inventor: **MITCHENKO, Valentin Alexandrovich**
[BY/BY]; Nekrasova Str., 28-210, Minsk, 220040 (BY).

(74) Agent: **VINOGRADOV, Sergey Gennadievich**; a/ya
114, Minsk, 220029 (BY).

LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK,
SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA,
ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian
patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European
patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,
IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF,
CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD,
TG).

Declaration under Rule 4.17:

— of inventorship (Rule 4.17(iv)) for US only

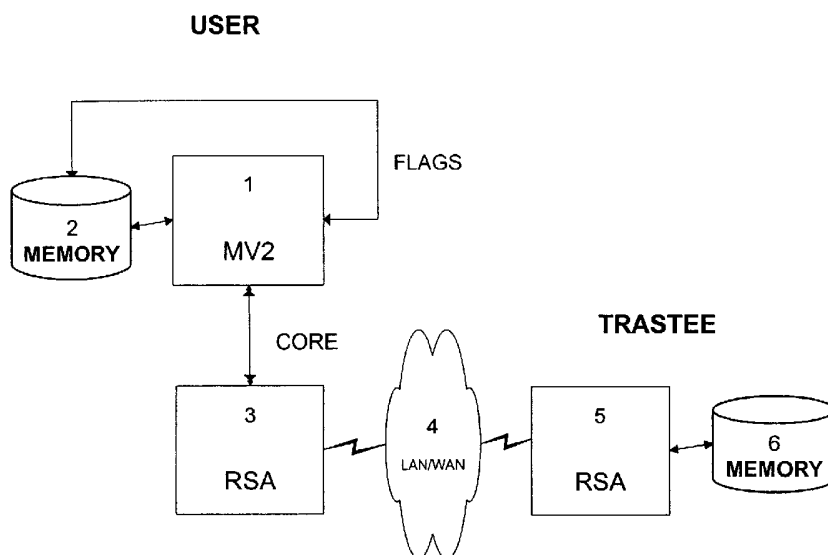
Published:

— with international search report

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD FOR SAFE STORAGE AND RESTORING OF INFORMATION



(57) Abstract: The invention relates to systems and methods providing centralized services for safe storage of secret information. An advantage of the present invention lies in the use of combination of encryption methods, when at least two independent parts of encrypted information are formed, and the RSA algorithm. This combination also provides reliable identification of users and the trustee allowing to organize a centralized system for safe storage of information. The claimed method allows to provide a high resistance encryption by means of performing a specified number of transformation cycles as well as by the resistance of the RSA algorithm. The methods allows to perform fast encryption with advantages of the RSA method.



WO 03/017565 A1

METHOD FOR SAFE STORAGE AND RESTORING OF INFORMATION

TECHNICAL FIELD

5 The invention relates to systems and methods providing centralized services for safe storage of secret information.

BACKGROUND

Brief review of cryptography

Cryptography is the process for encrypting or scrambling messages such that
10 the messages can be stored and transmitted securely.

Cryptography can be used to achieve secure communications, even when the transmission media (for example, the Internet) is public or untrustworthy.

Cryptography is also used by computer users for encrypting sensitive files, so that an intruder cannot understand them.

15 Cryptography can be used to ensure data integrity as well as to maintain secrecy.

Using cryptography it is also possible to verify the origin of data items, though the use of using digital signatures.

Generally, when using cryptographic methods, only the cryptographic keys
20 must remain secret. The algorithms, the key sizes, and file formats can be made public without compromising security.

Using data encryption, a data item can be scrambled so that it appears like random gibberish and is very difficult to transform back to the original data without a secret key. This message can consist of ASCII text, a database file, or any other
25 data.

The encryption and decryption keys are often, but not always, the same key.

There are two main classes of encryption algorithms: symmetric algorithms and public-key algorithms (also known as asymmetric algorithms).

Symmetric algorithms are the most common type of encryption algorithm.
30 They are known as symmetric because the same key is used for both encryption and decryption. Unlike the keys used with public-key algorithms, symmetric keys are frequently changed.

Compared to public-key algorithms, symmetric algorithms are very fast and, thus, are preferred when encrypting large amounts of data. Some of the more

common symmetric algorithms are RC2, RC4, and the Data Encryption Standard (DES).

Public-key (asymmetric) algorithms use two different keys: the public key and the private key. The private key is kept private to the owner of the key pair, and the public key can be distributed to anyone who requests it (often by means of a certificate). If one key is used to encrypt a message, then the other key is required to decrypt the message.

Public-key algorithms are very slow - on the order of 1,000 times slower than symmetric algorithms. Consequently, they are typically used only to encrypt session keys. They are also used to digitally sign messages.

One of the most common public-key algorithms is the RSA. This is a Public-Key Cipher.

Digital signatures can be used to distribute an unencrypted data item, while allowing the recipients to be able to verify that the message comes from its purported sender and that it has not been tampered with. Signing a message does not alter the message, it simply generates a digital signature string that can either be bundled with the message or transmitted separately.

Digital signatures are generated by using public-key signature algorithms: a private key is used to generate the signature, and the corresponding public key is used to validate the signature.

Authentication involves the process of verifying the identity of a person or entity. Certificates are a common way to achieve authentication. A certificate is a set of data that completely identifies an entity, and is issued by a Certification Authority.

Nowadays, financial and other sensitive transactions are being mostly performed by personal computers. Secret information and other data sensitive to intruder's access are stored in computers. This has increased the need for secure storage of information. Modern cryptography techniques are often used to protect such information from unauthorized access.

Generally, a method for data protection makes use of means allowing to store and protect "core" data secrets, such as private cryptographic keys, credit card numbers, and other small pieces of secret data. Presently, this responsibility is left to individual application programs or to personal computer users themselves. Although programs are available that allow users to encrypt and store data, such programs

cannot typically be used by other application programs. Currently, each application program has to devise a safe and secure method to store such data.

In addition, the encrypted data stored in the computer definitely are connected to the initial data and basically may be decrypted by selection of keys.

5 As an example of the problems associated with the current state of the art, consider the issues involved in exploiting smart card technologies. A smart card is particularly well suited as a receptacle for core data secrets such as those described above. In addition, smart cards can be used to authenticate users by requiring each user to insert his or her personal smart card into a receptacle associated with the
10 user's personal computer. Tamper-proof smart cards have been designed for just these purposes.

Problems arise without agreed-upon standards for using such devices. Although a developer could provide capabilities for working with a limited number of smart cards, it would be difficult or impossible to anticipate all the different variations
15 that might eventually arise. This fact makes it impractical to implement smart card technology in various different applications.

Although some storage media such as magnetic hard disks do not present the challenges of smart cards, many software developers simply do not have the background and knowledge required to safely implement modern cryptographic
20 techniques

Other methods require multiaspect manipulation and present challenges for the users without special background.

A method for encrypting disclosed in [WO 00/65767] is known. This method allows any machine text (any file), by repeated transformation with compression, to
25 be transformed into two encoded files, one of which is a product of repeated transformations (core). The second file represents information about the parameters of these transformations (flags) and has no meaning or connection with the initial text.

The feature of such representation is that one of the files (core) can have a
30 small size and a preset resistance (security) against an attack (that is selected by the user). Unlike the hash-function, the initial text (file) can be restored from the core file with the help of other file (flags) and special secret key information.

According to this method, transformation of a message in each cycle is performed in such a manner, as a result of which is formed a message (C_i)

transformed in the given cycle of transformation, which message is smaller in the length than the initial message, and the accessory information for the given cycle (F_i):

- the number (n) of transformation cycles of the initial message is selected from a preset criterion (for example, the size of the finally transformed message),
- 5 • an encrypted message consisting of two parts is formed, one of which contains the finally transformed message (C_n - core) that is smaller in the length than the initial message, and the second part contains a set of the accessory information ($F = \{F_1, F_2, \dots, F_n\}$ - flags).

This method for encryption allows the both parts of the encrypted message to
10 be independent from the initial text. In this case the initial text cannot be restored by any of these parts separately.

The drawback of this method is that when the both parts of the message are transmitted through one channel or stored in one place, they can be eavesdropped and restored illegally. In addition, often the user's authentication is required.

15 US patent № 6,044,155 " Method and system for safe archiving core data secrets" and US patent № 6,272,631 " Protected storage of core data secrets" are known.

The both inventions provide centralized storage for core data secrets referred to as data items. The architecture includes a storage server, a plurality of installable
20 storage providers, and one or more authentication providers. A default storage provider allows storage of data items on magnetic media such as a hard disc or a floppy disk or other media. Data items are encrypted by the user's computer by using the user's key which is derived from the user's password supplied during logon. The user's key is deposited by the network control computer such as a storage server.
25 The user sends the user's key to the server. The server adds to the key the user's authentication, which is at the same time transmitted to the authorized user of the user's computer and encrypts the resulting combination.

The encrypted combination is returned back and is locally stored by the user. For restoring the user's key the encrypted combination is sent to the server that
30 decodes the combination for deriving a data item. In this case the data item is returned to the user's computer only in case the decoded user's authentication matches the presently authenticated user of the user's computer.

Nevertheless, the core data stored in the computer have a direct relation to the initial data and, hence, can be unauthorizedly restored by selection of an
35 encryption key.

AIM OF INVENTION

The aim of the invention consists in providing a safe method for data storage protected from unauthorized access by using all advantages of communication media
5 and the Internet.

BRIEF SUMMARY OF INVENTION

The method for safe data storage and restoring comprises the following steps:

- deriving personal public and private key pairs for a user and a trustee;
- encrypting, in the user's computer the data secrets to be stored by an
10 encryption algorithm, as a result of which at least two parts of encrypted data (core and flags) are formed;
- additional encrypting at least one part of the encrypted data (core) by a trustee's public key;
- sending the part encrypted by the trustee's public key to the trustee's
15 computer, which authenticifies the received data by decoding the received part by the trustee's secret key;
- further encrypting the decrypted part by the user's public key;
- sending the part of the encrypted data, which was encrypted by the user's
public key, to the user's computer for authentication of the received data by
20 decoding the received part by the user's secret key for further restoring the initial data and matching the restored data with the initial data;
- confirming authenticity of the data part to be stored by the trustee;
- storing the decrypted data part by the trustee;
- storing the residue data part in the user's computer.

25

A method for recovering stored data comprises the steps of:

- requesting the data part stored by the trustee with the user's
authentication;
- encrypting the stored data by the user's public keys;
- 30 - sending the encrypted data part to the user;
- restoring the encrypted data part by the user's secret key;
- restoring the initial data from the restored data part (core) and the stored data part (flags) by reverse transformation;

The further improvement of the method is that if additional encrypting is
35 performed before sending to the trustee the part of the encrypted data, then during

data restoration respective additional decoding is performed in respect of the data part received from the trustee and restored by the secret user's key.

Still further improvement consists in that during restoration of the initial data, the said data are pre-restored from the part of additionally encrypted data received from the trustee and the part of the additionally encrypted data stored by the user and derived during first encryption, thereafter are restored the initial data from the pre-restored data part and from the data part stored after the first encryption.

10 BRIEF DESCRIPTION OF DRAWINGS

Fig. 1 shows a block-scheme of transforming initial data according to the invention.

Fig. 2 shows a block –scheme of transforming initial data with additional encryption of core part according to the invention.

15

DETAILED DESCRIPTION

Fig. 1 shows a scheme for data encrypting and storing according to the claimed method.

20 A method for secret transferring data comprises the following steps:

- performing by the user the first encryption 1 of the data to be stored in memory 2, in such a manner that two independent parts are formed: a content part (core) and an accessory part (flags), each of the said parts being unable to reproduce the initial data even in their separate parts;
- 25 • storing decrypted by 1 accessory part (flags) in the memory 2.
- additional encrypting 3 of the content part (core) by the user's individual public keys;
- transmitting the twice encrypted data part to Trastee through the network 4;
- decrypting 5 of the encrypted content part (core) 3 by the Trastee's private
- 30 keys;
- storing decrypted by 5 part in the memory 6.

Further improvement is that the main encryption 1 is performed in such a manner that the length of the content part is substantially shorter than the length of

the accessory part. Such a transformation can be termed as transformation with compression of the content part of data.

Preferably, the main encryption 1 is performed in such a manner that the content part has a fixed length (e.g. 1 KB) that is substantially shorter than the
5 accessory part.

A method for restoring initial data comprises the steps of:

- encoding 5 of stored in memory 6 of the content part of data by the user's public keys
- 10 • decoding 3 of the content part of data by the user's personal keys;
- restoring the initial data by performing the process of main decoding 2 by the interaction of the accessory part (flags) of data that carries information about transformation and the content part of data (core) that was pre-restored 3.

So, the claimed method uses the advantages of methods for encryption with
15 asymmetrical short part of data allowing at the same time to essentially improve the process of decoding on the account of encryption of the short part of data only. At the same time no unauthorized decoding of the rest (accessory) part of data is possible because it has no notional connection with the content of the initial text.

The stability(resistance) of such encryption is much higher, than in separately
20 taken methods, since the substantial part, being encrypted by asymmetrical keys is not subject to decoding as it has no semantic criterion.

At the same time, keys and the algorithm of the basic encryption can be also distributed through public channels. In this case the stability (resistance) of encryption will be determined by the stability(resistance) of the encryption under
25 RSA.

Moreover the length of RSA key in such case may be essentially more than standard (from 512 or 1024 bit up to 1 KB or more) and the total time for decryption of large files essentially decrease.

30 EMBODIMENTS OF INVENTION

It is preferable to use the method of encrypting information comprising the following steps:

- preliminary generating data about the ratios that connect the values of all initial symbols, which can be used in the given kind of information, with the encrypted
35 symbols.

- determining the number (n) of transformation cycles for each specific initial information;
- performing the transformation cycle, comprising:
 - generating the feature (R_i) determining the rule that is used for transforming the information in the current transformation cycle;
 - 5 transforming information with the use of the selected rule;
 - repeating the transformation cycles for a dedfinite number of times,
 - *while in this case*
 - transformation of information in each cycle is performed in such a manner that it results in forming the information transformed in the said cycle (C_i) and the accessory information for the said cycle (F_i);
 - 10 the number (n) for the transformation cycles of the initial information is selected from the preset criterion,
 - formation of encrypted information consisting of two parts, one of which includes the finally transformed information (core - C_n), and the second part includes the bunch of the accessory information ($F = \{F_1, F_2, \dots, F_n\}$).
 - 15

The method for data encryption can be characterized by the following features, in particular:

- transformation of information in each cycle is performed in such a manner, as a result of which is formed a transformed in the given cycle information (C_i) that is shorter in the length than the initial information or equal to it, and the accessory information for the given cycle (F_i);
- 20 • selection of the number (n) of the cycles for transformation of the initial information from the preset criterion that determines the length of the finally transformed information;
- 25 • formation of encrypted information consisting of two parts, one of which includes the finally transformed information (C_n) (core) that is shorter in the length than the initial information, and the second part includes the group of the accessory information ($F = \{F_1, F_2, \dots, F_n\}$) (flags).
- 30 • Further, the information (C_n) finally transformed at the given step is additionally transformed under the RSA method with the use of the public key of the asymmetric key pair of the recipient – data trustee.
- The finally transformed part of information (core) is transmitted to the trustee through one or several communication channels.
- 35

- To control the integrity and identity of the information transferred for storage, any standard procedure of verification may be used. In addition, for authentication of the subsequent inquiry of the stored information, a procedure of issue a certificate may be stipulated, or an identification record may be added to the stored information.
- Separate storage of the encrypted data parts reduces the opportunity of interception or matching the parts and, consequently, increases the stability(resistance) of the system for data storage, since each part of information in itself has no meaning.
- In this case a high degree of privacy is provided since both parts of the encoded data are never transferred together, being stored most of the time separately. Moreover, the algorithm and keys of the preliminary encryption can be generated randomly each time and stored in the user's computer. In this process neither keys, nor flags have any semantic connection with the initial text. In this case the stability(resistance) of the system will be determined by the stability(resistance) of the algorithm, which may be set as much as high depending on the number of cycles of transformation and on the length of RSA keys. However, unlike common RSA system, such system is much faster. In addition, the stability (resistance) of the preliminary encryption algorithm even with public keys is rather high, since it is determined by the length of the compressed data part, which may be rather long, e.g. 1 Kilobyte.

The method for decoding the encrypted data comprises the steps of:

- requesting, by the user of the data part stored by the trustee;
- encrypting the requested data part by the user's-recipient public keys;
- sending by the trustee and receiving by the recipient of the encrypted stored data part;
- pre-decoding, by the RCA algorithm and the secret key of the asymmetrical key pair of the recipient, of the essential part of the encrypted message that was additionally encrypted by the sender by means of the public key of the asymmetrical key pair of the recipient.
- generating the keys for pre-encryption that are identical to the rules used during pre-encryption;
- extracting from the encrypted information the data (R_i) that determin the rule used in the current transformation cycle, which rule connects the values of the

encrypted information with the specific symbols of the transformed information of the current transformation cycle;

- selecting the rule connecting the values of the encrypted information with the specific symbols of the transformed information of the current transformation cycle;
- extracting, from the accessory information (F), the accessory information for the given transformation cycle (F_i);
- transforming the transformed information (C_i) with the use of the selected rule and the accessory information for the given transformation cycle (F_i);
- making decision about transition to the subsequent cycle or about termination of transformation;
- *while in this case*
- the accessory information for the given transformation cycle (F_i) is selected from set of the accessory information (F);
- the transformed in the respective cycle information (C_i) is restored with the use of the selected rule and the accessory information for the given transformation cycle c (F_i);
- the decision is made about transition to the subsequent cycle or about termination of transformation;
- the respective part of the accessory information is additionally used in each transformation cycle; a restored in the respective cycle information is formed as a result of transformation with the use of the selected rule.

Accordingly, the cycles are repeated up to full restoration of the initial information.

Fig. 2 illustrates further improvement of the method.

Still further improvement of the method allows to perform one more transformation 7 of the encrypted data part that is to be sent. All other operations are the same as on Fig.1.

In this case, it is possible to use the similar algorithm with formation of a "core" and "flags". Thus, the trustee receives only the secondary "core" sent according to the appropriate procedure with asymmetrical keys. The rest part (secondary flags) is stored in the memory 2 of user's computer. In this case the length of the message sent for storage can be essentially reduced without any decrease of resistance of protection, but even with increase thereof.

Accordingly, during decoding it is necessary to perform the procedures of additional decoding 7 that are similar to the former one, but are carried out in the reverse order.

5 This method allows to provide the encryption resistance by means of the number of transformation cycles, by a key length as well as by the resistance of the RCA algorithm.

Essential advantage of the present invention also lies in the combination of the first method of encryption with the RSA algorithm. This combination also provides reliable identification of users and the trustee allowing to organize a centralized
10 system for safe storage of information.

Conclusion

The feature of the claimed method versus the prior art inventions also consists in that only short nucleus are stored in the centralized depot, while the basic volume of data is stored at the user. Thus, the part stored at the user has no semantic
15 connection with the initial text, therefore it cannot be restored by any unauthorized user. For the trustee the short essential data part also is meaningless, since the resistance of this part is determined by the length of the accessory part comparable with the initial text, and by the amount of transformation cycles, which may be set arbitrary large. Thus, it is possible to regard the said method as having a practical
20 resistance.

1. A method for safe storage of information comprising the steps of:
- generating individual public and secret pairs of keys for a user and for a trustee;
 - 5 – encrypting in the user's computer the initial information to be secretly stored;
 - storing the encrypted information in the user's computer;
 - additional encrypting, by the public key of the trustee, the secret data of the first encryption procedure;
 - 10 – sending the secret data encrypted by the trustee's public key to the trustee's computer;
- characterized in that
- the encryption of the initial information in the user's computer is carried out by means of an encryption algorithm, as a result of which at least two parts
 - 15 of the encrypted information are formed;
 - additional encryption is performed by the public key of the trustee at least for one part of the encrypted information;
 - the part of the encrypted initial information that was encrypted by the public key of the trustee is sent to the trustee's computer;
 - 20 – a part of the received information is decoded by the trustee by means of his secret key;
 - the decoded part of information is stored by the trustee;
 - the decoded part of information is further encrypted by the public key of the user;
 - 25 – the part of the information encrypted by the public key of the user is sent to the user's computer;
 - the received part of information is decoded by the user by means of the user's secret key;
 - the received information is authenticated by matching the recovered
 - 30 information with the sent encrypted part of information.

2. A method of claim 1, characterized in that prior to performing encryption by the public key of the trustee, a part of the encrypted initial information is additionally encrypted and then sent to the trustee. .

3. A method of claim 1, characterized in that the additional encryption is performed by means of an encryption algorithm, as a result of which at least two parts of encrypted information are formed;

5 – at least one part of the additionally encrypted information is additionally encrypted by the public key of the trustee;

 – the encrypted part of the additionally encrypted information that was encrypted by the public key of the trustee is sent to the trustee, while the part of information remaining as a result of additional encryption is stored by the user.

4. A method for restoring stored information comprising

10 – requesting the part of information stored by the trustee with the user's authorization;

 – encrypting the stored information by the public keys of the user;

 – sending the encrypted part of information to the user;

 – restoring the encrypted part of information by the secret key of the user;

15 – restoring the initial information from the restored part of information(core) and the stored part of information (flags) by means of reverse transformation.

5. A method of claim 4, characterized in that if prior to sending a part of the encrypted information to the trustee, an additional encryption is performed, then, respectively the part of information, received from the trustee and recovered
20 by the secret key of the user, is additionally decoded.

6. A method of claim 5, characterized in that during recovering the initial information, from the part of the additionally encrypted information received from the trustee and from the part of the additionally encrypted information stored by the user, preliminary is recovered the part of information formed as a result of first
25 encryption, thereafter the initial information is recovered from the pre-recovered part and the part stored after the first encryption.

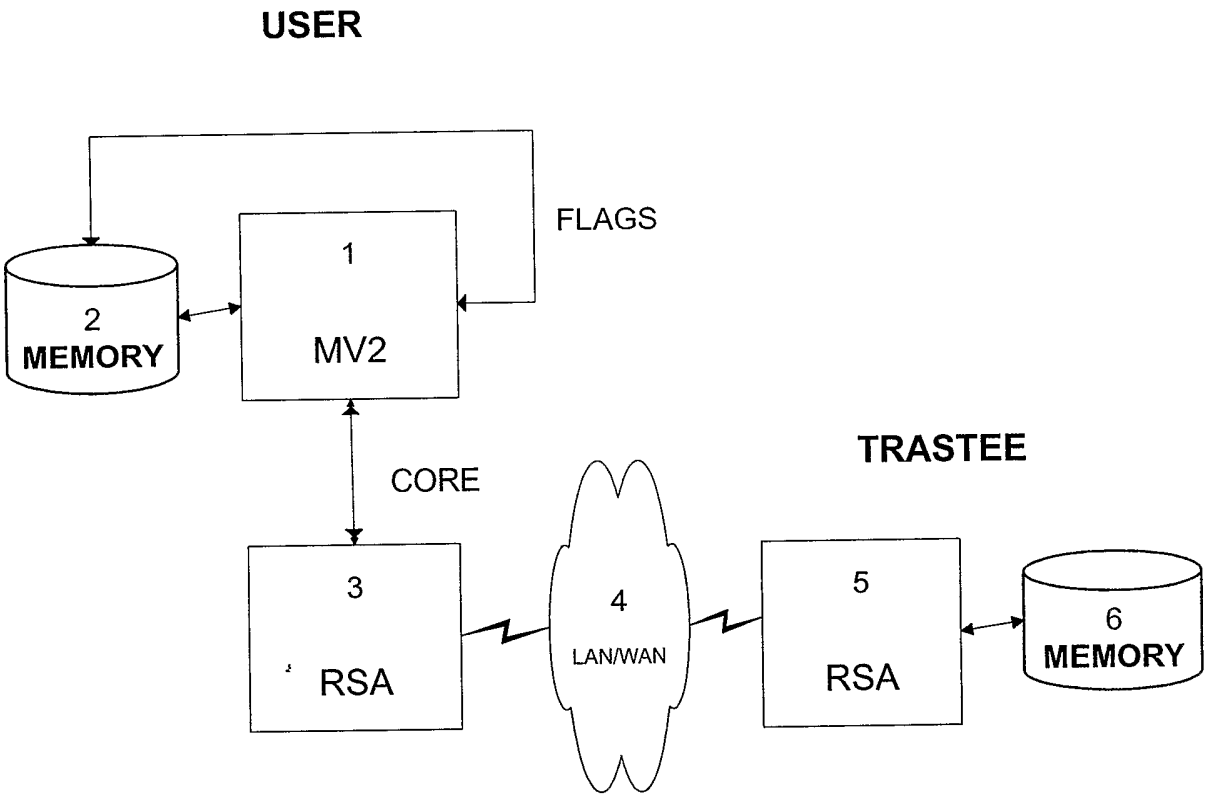


Fig. 1

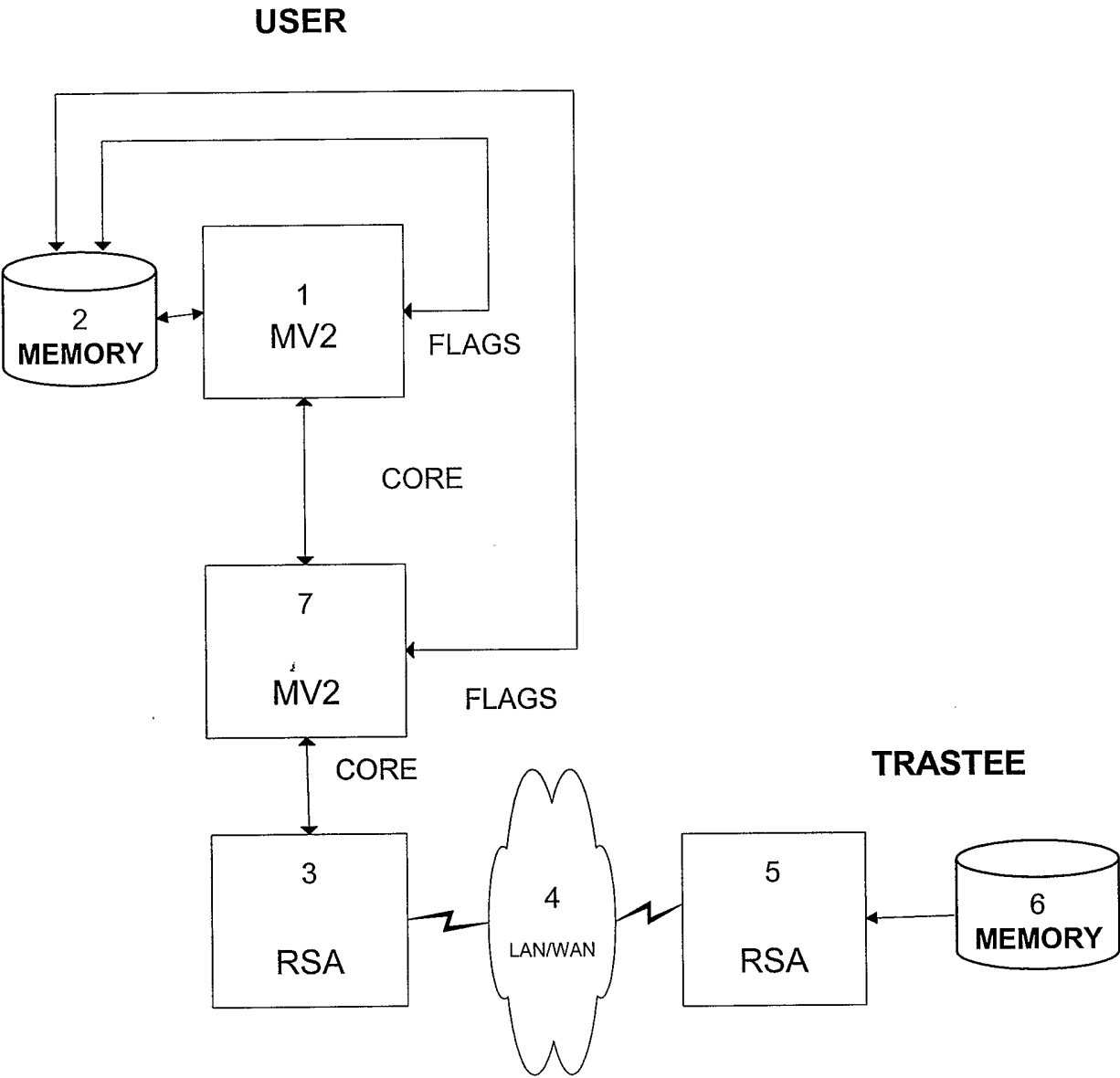


Fig. 2

INTERNATIONAL SEARCH REPORT

International Application No

PCT/BY 01/00012

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00 65767 A (VERZHBALOVICH DZMITRY I ;VILANSKI YURI V (BY); MISCHENKO VALENTIN) 2 November 2000 (2000-11-02) cited in the application page 5, line 7 - line 25; claim 1 ---	1
A	EP 0 912 011 A (SUN MICROSYSTEMS INC) 28 April 1999 (1999-04-28) abstract column 4, line 48 -column 8, line 29 -----	1,4

☐ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

& document member of the same patent family

Date of the actual completion of the international search

17 May 2002

Date of mailing of the international search report

06/06/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/BY 01/00012

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0065767	A	02-11-2000	WO 0065767 A1	02-11-2000
			AU 3922299 A	10-11-2000
			EP 1171970 A1	16-01-2002
EP 0912011	A	28-04-1999	US 6160891 A	12-12-2000
			CA 2251193 A1	20-04-1999
			EP 0912011 A2	28-04-1999
			JP 11215117 A	06-08-1999