(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 August 2007 (16.08.2007)

PCT

(10) International Publication Number
WO 2007/091002 A1

(51) International Patent Classification:
G06F 21/24 (2006.01)

(21) International Application Number:
PCT/GB2006/001766

(22) International Filing Date: 12 May 2006 (12.05.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
183/MUM/2006 7 February 2006 (07.02.2006) IN

(71) Applicant *(for all designated States except PG, US)*: **NEXTENDERS (INDIA) PRIVATE LIMITED** [IN/IN]; Yuchit, Juhu Tara Road, Mumbai 400049 (IN).

(71) Applicant *(for PG only)*: **ZOOM CORTEX LIMITED** [GB/GB]; Carnisla 2B, Aldersey Road, Guildford GU1 2ES (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SHEVADE, Ravindra, Waman** [IN/IN]; D-01, 403 Santoor, Lokpuram, off Pokhran Road No. 2, Thane, Maharashtra 400 601 (IN).

(74) Agents: **DeVILE, Jonathan, Mark** et al.; D Young & Co, 120 Holborn, London EC1N 2DY (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

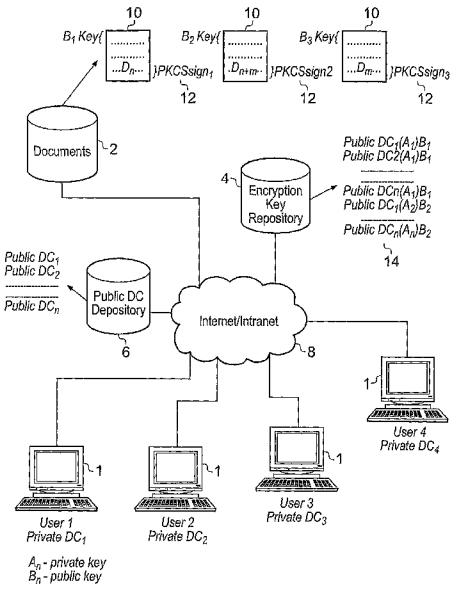
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *as to non-prejudicial disclosures or exceptions to lack of novelty (Rule 4.17(v))*

Published:
— *with international search report*

[Continued on next page]

(54) Title: DOCUMENT SECURITY MANAGEMENT SYSTEM



(57) Abstract: A document security management system for securely managing documents for users. The document management system comprises a document repository providing a facility for storing data files representing the documents. A key repository stores a public key of one or more encryption key pairs, each of the encryption key pairs being associated with one of the documents stored in the document repository. Each document stored in the document repository is encrypted with the public key of the encryption key pair associated with the document. A plurality of client terminals are operable to store and to retrieve the documents from the documentary repository for processing by a user. Each user is in possession of a digital certificate comprising a certificate key pair. The key repository includes the private key of the encryption key pair encrypted with the public key of the certificate key pair associated with the user. The client terminal is operable with the private key of the certificate key pair in possession of a user. The client terminal is operable to decrypt the private key of the encryption key pair using the private key of the certificate key pair of a user, and to retrieve the encrypted document from the document repository and to decrypt the document using the decrypted private key of the encryption key pair. Thus, in accordance with the present invention a two tier arrangement of private key/public key pairs is provided with a first private key/public key pair called the encryption key pair being associated with each of the documents and a second digital certificate private key/public key pair called a certificate key pair being associated with the users. A document management system according to the present invention is therefore provided with an improvement in security with respect to document management and document management security.

WO 2007/091002 A1

— *with a declaration as to non-prejudicial disclosures or exceptions to lack of novelty*

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.

DOCUMENT SECURITY MANAGEMENT SYSTEM

Field of Invention

The present invention relates to document security management systems for securely managing documents for users.

In one embodiment a document security management system is provided on a client-server arrangement, in which client terminals are interconnected via a telecommunications network to one or more servers.

Background of the Invention

There is an increasing requirement to improve the security with which corporate information is stored and used in digital form. Documents and information may contain any type of data, scanned images, program files, text or databases, which are stored as data files on a document repository server. Whilst it is known that information and document management systems can include some measure of access and privilege control, critical information may remain unencrypted and/or accessible to system administrators, database administrators and backup media managers.

It is desirable to provide a system with improved security management of documents or data stored on the system.

Summary of the Invention

Various aspects and features of the present invention are defined in the appended claims.

Embodiments of the present invention can provide a document security management system for securely managing documents for users or for securely managing data for users. The document security management system comprises a document repository (which could be any industry standard or proprietary format repository) providing a facility for storing data files representing documents and a separate secure encryption key repository for securely storing public-private key pairs ("encryption key pairs") which are used to encrypt and decrypt documents in the document repository. Each of the encryption key pairs is associated with one or more of the documents currently stored or intended to be stored in the document repository.

Each document stored in the document repository is encrypted with the public key of a specific encryption key pair ("encryption public key"). Hence there is for every document in the repository an associated encryption key pair (as distinct from a digital signature certificate key pair) stored in the secure encryption key repository. A plurality of client terminals are operable to retrieve the encrypted documents from the document repository for processing or viewing by users. Each user needs to obtain a digital signature certificate which contains a user-specific private key-public key pair, which may be for example in accordance with generally accepted National and International standards of PKI and National Legislation. The private key associated with a digital signature certificate key pair ("certificate private key) is accessible only to the owner of the certificate by commonly accepted PKI standards.

The key repository stores the private key of the encryption key pair ("encryption private key") encrypted with the public key of the digital signature certificate key pair ("certificate public key) associated with a user. The repository can contain for each document plural copies of the document's associated encryption private key, one separate copy per authorised user, with each user's encryption private key copy encrypted with that user's certificate public key. The repository also contains a single copy, in unencrypted form, of the encryption public key of each encryption key pair and a single copy of the certificate public key of each registered user of the system.

The client terminal has access to the user's certificate private key by virtue of having the digital signature certificate installed on the client terminal or through an attached device. The client terminal is operable to obtain a copy of the encryption private key from the key repository and to decrypt the encryption private key using the certificate private key to retrieve the encrypted document from the document repository and to decrypt the document using the encryption private key associated with the document. The obtained encrypted encryption private key is typically not deleted from the key repository.

Embodiments of the present invention can use industry-standard two key encryption algorithms such as RSA and address the following limitations of basic two-key encryption / decryption technology:

- A single encrypted copy of a document can be made available to multiple users in encrypted form with a reduced likelihood of compromising document security and without reliance upon transferring digital certificates;
- Controlled access to documents can be provided without relying a requirement for allocating and revoking personal digital certificates;
- Transfer of access privileges from one user to another can be provided without a requirement for decrypting the documents and without a need for users whose access is being removed being involved in the access privilege transfer;
- Document updates and document edits can be tracked and in particular View Access (i.e., those who have viewed the document even without saving, editing, or updating it in any way) and a legally certifiable record can be maintained, for example using PKI encryption of access to the document with a time stamp;
- Storing or transmitting copies of unencrypted keys with third parties and escrow agents is not typically required and the use of an escrow master key for any of the purposes stated above is not required.
- Since digital certificates have a limited validity, issue and management of multiple digital certificates per user can be handled independent of the security management system.

The document security management system according to an example embodiment of the present invention is provided with a document repository for storing data files, where each file has been encrypted with an encryption public key. The encryption public keys are stored in the key repository but in an unencrypted form. However the encryption private key, also stored in the key repository, is encrypted with the certificate public key associated with a user. As such, documents and encryption private keys are neither stored unencrypted nor communicated unencrypted. Decryption of the encrypted encryption private key only takes place in the client terminals by the provision of the certificate private key, which is allocated to the user and then the decrypted encryption private key is used to decrypt the encrypted document in the client terminal. That is to say, that the certificate private key is used

to decrypt the encryption private key to recover the encryption private key. This is then used to decrypt the encrypted document, which has been encrypted with the encryption public key. To enhance security, the decrypted encryption private key is discarded soon after or immediately on decryption of the document and is not stored in the client machine. If necessary the encryption private key can be once more downloaded and decrypted by the user since it is only a copy of the encrypted encryption private key that has been retrieved on the client terminal.

Thus, in accordance with the present invention a two tier arrangement of private key/public key pairs is provided with an encryption key pair being associated with each of the documents and a second digital certificate key pair being associated with the users. A security management system for documents according to the present invention is therefore provided with an improvement in security and security management with respect to data files representing documents, which are managed by the system.

If a user leaves the organisation then his/her access to an encryption key pair can be withdrawn by simply deleting the user's encrypted copy of the encryption private key from the repository. In some embodiments the key repository is arranged to store each of the encryption private keys of the encryption keys pairs, encrypted with the certificate public key of one or more key managers. The key manager can therefore access the set of encryption private keys which had been allocated to a user (each encryption private key representing a unique document stored in the document repository), and remove one or more of the encryption private keys from the user's section of the key repository and if appropriate allocate it to another user. Accordingly, security is maintained even if a user leaves an organisation which operates the security management system for its documents.

Embodiments of the present invention may also be arranged to generate a hash value of the document after the document has been created or edited by a user. A hash value is a form of document digest, which represents in digital form the content within a data file. A client terminal on which a document has been created and/or edited may be arranged to run an application to generate the hash value. The client terminal may also generate a detached signature, which may be formed using the hash value. As such, when the user again edits the document the client can confirm that the document

has not been amended in that the document corresponds to the hash value and that the signature corresponds to that generated when the document was previously signed by the user or the last user to edit the document. Accordingly, a further improvement in security is provided. In one example, the signature is a Public-Key Cryptographic Standards 7 (PKCS7) signature.

In some embodiments the document repository may include a log identifying when documents are retrieved for editing and/or viewing. As such management of documents and tracking of changes of secure information is thereby facilitated.

Various further aspects and features of the present invention are defined in the appending claims.

Brief Description of the Drawings

Embodiments of the present invention will now be described by way of example only with reference to the accompanying drawings where like parts are provided with corresponding reference numerals and in which:

Figure 1 is a schematic block diagram of a document management system in which a plurality of client terminals are connected to a document repository and to a key repository;

Figure 2 is a flow diagram illustrating a process through which an encryption key pair is generated and stored in the key repository server shown in Figure 1;

Figure 3 is a part block diagram part flow diagram illustrating a process through which a document is created on a client terminal;

Figure 4 is a part block diagram part flow diagram illustrating a process through which a document is accessed and edited on a client terminal;

Figure 5 is a flow diagram illustrating a process by which a new digital certificate private key/public key pair is issued and the public key is stored on a public key digital certificate repository shown in Figure 1;

Figure 6 is a flow diagram illustrating a process by which a user updates a copy of an encryption key pair after expiry of a user's digital certificate; and

Figure 7 is a flow diagram illustrating a process by which existing key pairs are issued to a new user.

Description of Example Embodiments

Example embodiments of the present invention will now be described with reference to Figure 1 which provides a schematic illustration of a security management system for documents which may for example be installed in an organisation where some level of security is appropriate to control, distribution and disclosure of information. In Figure 1 a plurality of client terminals 1 are connected to a document repository server 2, a key repository server 4 and a public digital certificate repository server 6 via a communications network 8. The document repository 2 is arranged to store information in the form of data files 10. However, each of the data files is encrypted with a public key of one of a plurality of encryption key pairs (A-key/B-key for encryption private key and encryption public key respectively). Thus each of the documents 10 has associated therewith one or more encryption key pairs.

In Figure 1 the encryption key pairs are designated A_nB_n. Thus for a first of the documents shown the document 10.1 is encrypted with the public key B_1 of one of the encryption key pair A_1B_1.

The documents may also include a digital signature 12. As will be explained in the following paragraphs, the digital signature is added once a user has accessed the document or created the document.

As well as the encryption key pairs, the document security management system also includes a plurality of digital signature certificate key pairs which form digital certificates. These will be referred to in the following description as certificate key pairs (certificate private key or certificate public key as the case may be). Each of the plurality of certificate key pairs is associated with one of the users of the system. Thus, for the example shown in Figure 1 each of the client terminals has a user associated therewith (although a user may operate from any terminal carrying his digital certificate and certificate private key with him on a hardware device attachable to any terminal) and each user has associated with it a certificate key pair. A user may actually operate from any terminal carrying his/her certificate private key on an attachable mobile hardware device such as a smart card, USB token, mobile phone, PDA, etc. However it will be appreciated that there could be more users than client

terminals and therefore the security management system is not limited to four certificate key pairs. The public keys of the certificate key pair are stored in public digital certificate repository server 6.

The encryption key repository server 4 stores the public key and the private key of the encryption key pairs. As mentioned above there is an association between the encryption key pairs and the documents present in the document management server 2 such that for each such document there is one and only one encryption key pair associated with it. However, a particular encryption key pair may be associated with more than one document. For example, if a set of related documents all require a common group of users to access the set then one can assign just one encryption key pair to each document in the set. Note that other relationships are:

- Multiple users may have access to the same encryption key pair
- Multiple encryption key pairs may be accessible by the same user
- Each certificate key pair is assigned to one and only one user
- Each user may have multiple certificates (e.g., expired certificates are still required for signature verification and hence a user may collect many certificates over a period of time, each however uniquely assigned the that user alone)

More than one user may have access to any one document. Furthermore different users may be allowed access to the same document whilst maintaining security and uniquely identifying actions of one user with respect to those of another. To this end, each of the private keys of the encryption key pair associated with a document is encrypted with the public key of the certificate key pairs of users who may be allowed access to the document. Thus each private key of an encryption key pair associated with a document is encrypted with the public key of the digital certificate. Any user having access to that document therefore has an encrypted version of the private key, this encryption private key being encrypted with the public key of that user's digital certificate. Thus, as shown within an area 14 within Figure 1, for each document and for each user which has access to that document there exists a public key for the encryption key pair. There also exists the private key of the encryption key pair encrypted with the public key of the certificate key pair.

According to the example of the present technique a key manager (or multiple key managers in other embodiments) manages the distribution of the encryption key pairs to the various users and manages the repository of public keys of certificate key pairs. Each user obtains his/her digital certificate from a legally valid Certifying Authority and sends his/her public key of the digital certificate to the key manager. For example, governments have incorporated national legislation to govern and regulate certifying authorities, thus providing legal sanctity to digital certificates issued by them. The key manager uses a public digital certificate repository 6 to store the certificate public keys. In one example the private key of the certificate key pairs are provided on smart cards which can then be used in a smart card reader when the user is accessing one of the client terminals 1.

As explained above the encryption key pairs comprise two asymmetric pairs, which are represented in Figure 1 as a B-key which is the shorter public key and the A-key which is the longer private key. Each pair is also provided with a unique identifier (key pair ID or key ID). Data files representing documents stored in the document repository 2 are always encrypted with the B-key (encryption public key) of the key pair. The key pair ID of the B-key that is used for encryption is stored along with the encrypted data file. Therefore it is always possible to know given an instance of the encrypted data file, which encryption key pair is to be used for decrypting the information and/or encrypting the information provided in the data file. Users are granted specific access to review and/or update the data files. The data files are updated and then re-encrypted in the client terminal before being communicated back to the document repository 2.

The document repository 2 may contain structured data files or digital files or both. The key repository 4 stores the encryption key pairs. The B keys are stored in unencrypted form and all A-keys are stored in encrypted form. In one example, the encryption key pairs are generated by the user who has created the document. Alternatively, encryption key pairs may be created by a key manager within the organisation. There can be multiple key managers within a given organisation, who are responsible for different sets of encryption key pairs. Each authorised user has access to all public keys (B keys) of the encryption key pairs, because these are unencrypted. Each user may have access to multiple private keys of the encryption

key pairs (A-keys) which are stored in a user specific section 14 encrypted with the public key of the user's digital certificate. A process through which the encryption key pairs are generated is described in the following section.

Encryption Key Pair Generation

Figure 2 provides a flow diagram representing a process in which an encryption pair is generated by a user in association with a document. Figure 2 is summarised as follows:

S1: The user applies a key generation application which is operating, for example, on the client terminal on which the user is working in order to generate an encryption key pair. A private encryption key is never available on the server in unencrypted form. It is available on client terminal in unencrypted form only while the session with the server is live during which period only the authenticated user has access to that client terminal.

S2: The private key (A-key) of the encryption key pair is then encrypted (at least) twice – one copy is encrypted with the user's digital certificate public key and a second copy with the key manager's public key. The private key (A-key) of the encryption key pair is encrypted with the key manager's public key so that the key manager can decrypt the private key (A key) should this be necessary if the user were to leave the organisation or has to be denied access to that document for some reason.

S4: The user then updates the key repository server with a public key (B-key) and the encrypted private key (A-key) of the encryption key pair.

S6: Optionally the key manager may issue the public key (B-key) and the private key (A-key) to the user, if the key manager generated this encryption key pair. The private key (A key) is encrypted with the public key of the user's certificate key pair. The key manager may then authorise other users to access the document by encrypting copies of the private key (A key) of the encryption key pair with the public key of the other users' certificate key pair.

The key pair generation may take place when a document is generated or may be generated before a document is first created, but in all cases before the document is updated / sent to the server so as not to compromise security.

Adding Secure Information to the Document Repository

Figure 3 provides a part-schematic, part-flow diagram illustrating a process through which a user creates a document and then stores the document in encrypted form in the document repository using the encryption key pair generated in Figure 2. In Figure 3, one of the client terminals 1 is used by a user, for example user2, to create a data file 20 representing a digital document. The data file is created by an application program running on the client terminal 1 in a conventional manner. An application on the client terminal then generates a digital hash using, for example, the Secure Hash Algorithm SHA-1 of the data file at a first step 22. The application also then generates a detached digital signature 24, which is generated using the digital certificate of the user. Thus, the digital signature is generated by the user using the user's private key of the digital certificate from the document. The digital signature uses the private key. It serves as a signature because it is based on the private key to which only the owner of the certificate has access. In one example the digital signature is a Public-Key Cryptography Standards # 7 (PKCS7). The PKS7 signature is then attached to the digital document 20. More information on the PKCS7 can be found from the RSA Laboratories (www.rsasecurity.com).

The application on the client terminal 1 then retrieves the public key of one of the encryption key pairs which has either been pre-generated as indicated above or is generated at the time of creation of the document 20. The key repository 4 provides the public key (B_x key) 26 to the client terminal 1 which is used to encrypt the document data file 20 to form an encrypted data file 20′, the document having been encrypted with the public key of the encryption key pair.

The encrypted data file 20′ is then stored in the document repository server 2 by communicating the encrypted data file from the client terminal 1 to the document repository server 2 via the communications network 8. The document is communicated with the digital signature (PKCS7). Furthermore, the hash value is included with the communicated encrypted data file 20′. Thus the document repository server stores the data file 20 in encrypted form (encrypted with the public key of the encryption key pair) with the hash value included in the digital signature.

Secure Access Log

According to the present technique whenever a user accesses a document then he/she is required to generate a digital signature which is communicated to the document repository server and stored in association with the document concerned. As indicated above, in one example the digital signature is generated in accordance with the PKCS7 international standard for generating digital signatures. In one example, the digital signature is a detached digital signature. The digital signature will always include the public key (B-key) associated with the document, that is the public key of the encryption pair allocated to that document required for recording an attempt to access the corresponding private key, and will always include the hash value generated from the document which is encrypted with the private key of the certificate key pair of the user accessing the document. As mentioned above the hash value forms a digest of the content of the data file representing the document. Since the encryption public key is available on the key repository server 2 then any authorised user can download the appropriate public key and verify the signature by decrypting the encrypted hash value with the public key of the certificate pair in order to validate the viewed signature.

Viewing Secure Information from Repository

Figure 4 provides a part-schematic block diagram of the system elements and a part-flow diagram illustrating process steps involved in viewing and editing documents stored on the document server 2. In Figure 4 a user, for example user Y, accesses one of the client terminals 1 in order to review and/or edit a document stored on the document server 2. The process steps performed in order to view and edit a document are summarised as follows:

S10: The user Y first activates an application program on the client terminal, which sends a request for information to the document server 2 requesting access to a particular document. Prior to the request the user authenticates itself as an authorised user by decrypting with its certificate private key a random challenge phrase sent by the server, the server having sent the challenge phrase encrypted with the public key of the user's digital certificate.

S12: For the requested document, the document repository server 2 finds the key pair ID of the encryption key pair corresponding to the document identifier D_n. The document server 2 then checks the record of user Y with respect to the encrypted private key of the encryption key pair identified by the key ID associated with the document identifier D_n. If user Y's record is not found for the specific Key Pair ID, request is rejected.

S14: If user Y's record is found, the document server 2 obtains the private encryption key corresponding to the public key with which the document concerned has been encrypted from the key repository and then sends it to the user. The private key (A_x) is sent to the user in a form in which it has been encrypted with the public key of the digital certificate of the user Y 40.

S16: The document server 2 also sends the identified document 52 to the user which, as previously mentioned, is encrypted with the public key of the private key/public key pair.

S18: Together with the encrypted data representing the document 52 a digital signature is also sent with the data file representing the document 52 to the client terminal 1, which is communicated to the user terminal 1 in response to the request for the document D_n.

Once the user terminal 1 receives the encrypted document 52 the application on the client terminal 1 performs the following functions as indicated within an area 54 illustrating the functional steps performed by the application program:

S20: The application on the client terminal 1 decrypts the private key (A-key) of the first private key/public key pair received from the document repository server 2 using the private key of user Y's digital certificate.

S22: The client terminal 1 then decrypts the document 52 using the decrypted private key (A-key) of the first document private key/public key pair associated with the document 52.

S24: The application program running on the client terminal 1, then generates an SHA1 hash of the decrypted document 52.

S26: The generated hash value is then compared with the hash value obtained by decrypting the hash in the PKCS7 detached signature of the previous user

X with public certificate key of user X which was received with the decrypted document 52 from the document server 2. This establishes that X's signature is valid and the document has not been viewed/accessed/changed by anyone between the time X accessed it and now.

S28: The application program then generates the PKCS7 detached digital certificate for user Y. The signature is generated by encrypting the hash value with the public key of the user Y's digital certificate.

S30: The application on the client terminal then sends the PKS7Y signature generated by the user Y from the client terminal 1 for storage on the document server 2.

S32: The client terminal sends the key ID of the encryption key pair, which was used to encrypt the document. The document ID and the date and time at which access took place are also sent for storage in the document server 2. To increase security, by reducing a likelihood of the key ID, the document ID or the date and time being altered by an attack which is aimed at disrupting the document management system the key ID, the document ID and the date and time are encrypted with the private key of the user Y's digital certificate.

S34: As illustrated by an arrow, the key ID, the document ID and the date and time are sent to the document server 2 for storage. The key ID and the document ID are digitally signed by the user's digital certificate to create a "view signature" with the date and time. This provides a unique identifier indicating when the document was reviewed, edited and accessed. The hash value is also used by the viewing user to verify the authenticity of the signature, which the user is creating. The "view signature" is updated on the document server 2 along with a view log. Once the document has been edited it is then re-encrypted and stored on the document repository with a new hash value and a new view signature as represented by the flow diagram in Figure 3.

If a different user wishes to access the same document then a second version is stored. Information stored by a previous user is not updated, except for adding the "view signature" of the current user.

When a user leaves an organisation or is no longer to be allowed access to certain information the corresponding private keys (A keys) associated with the

encryption key pairs are removed from this user's section of the key repository and, if appropriate and necessary, allocated to a different user. When the private key of the encryption key pairs are allocated to a different user, that user views the information as set out above and digitally signs the information after verification. A second detached PKS7 signature is stored on the server and associated with the document for which that user is now responsible.

The document management system according to the present technique can also be extended to deny access to any single user or even multiple users when access to certain secure information is to be granted only if some or all of a set of authorised users are physically present logged in (frequently required for security reasons or as company policy). The private (A-key) of the first document private key/public key pair is not issued to a single user as a whole but is split into two, three or a plurality of parts as required and individual parts are assigned to specific users. In this example, all users who hold parts of the key have to log in together (in any order) from the same client terminal and apply their digital certificates (or smart card and/or through typing a password) before the information can be decrypted.

Addition of a New Digital Certificate Public Key on Public DC Repository

To acquire a new digital certificate private key / public key pair for accessing encrypted documents in accordance with the present technique, a user would in one example apply to a certifying authority for a new digital certificate public key / private key pair. After being provided with the new digital certificate public key/private key pair the user then up-dates its digital certificate by sending the public key to the key manager. A flow diagram illustrating an example of this process is shown in Figure 5. The process steps of Figure 5 will now be summarised as follows:

S40: A user generates a new private key / public key pair on a client terminal. The new private key / public key pair could be generated on a smart card or on a USB token or may be generated on a personal computer (for example a note book PC) which forms the client terminal. The user then sends the generated public key of the digital certificate pair along with a request to a certifying authority for issuing a new digital certificate which could be either an additional digital certificate private key

/ public key or a renewal of an existing digital certificate. The user completes the necessary identification verification formalities to satisfy the certifying authority.

S42: The certifying authority then validates the request from the user and generates a new digital certificate containing the user's new certificate public key, signs the digital certificate with the certifying authority's private key and sends the new digital certificate to the user. On receipt of the new digital certificate the user checks the certifying authority's certificate and installs the digital certificate on the client terminal.

S44: The user then sends the public key of the new digital certificate to the key manager of the organisation with a request to add the key to the public digital certificate repository. The user also sends the existing digital certificate public key whether valid or expired, the public key being currently stored in the public digital certificate repository.

S46: The key manager then authenticates the user by checking the certificate public key currently stored in the public digital certificate repository with the existing digital certificate public key sent by the user. The key manager then also validates the new digital certificate by checking this digital certificate with a third party revocation list for example provided by the certifying authority.

S48: The key manager stores and updates the user's certificate public key of the new digital certificate on the public digital certificate repository.

Updating a User's Copy of an Encryption Key Pair after expiry of a User's Digital Certificate

The process through which a user updates a copy of an encryption key pair using the new digital certificate acquired in the process illustrated above is represented in Figure 6. The flow diagram shown in Figure 6 is summarised as follows:

S50: The user updates the public digital certificate repository with a new certificate public key as for example illustrated by the steps of the process illustrated in Figure 5.

S52: The user first downloads the copy of the encryption private key from the encryption key repository, which is encrypted with the user's old public key.

S54: The user then decrypts the encrypted private key (A key) using his old digital certificate private key to recover the encryption private key (A key).

S56: The user then re-encrypts the decrypted encryption private key (A key) with the new digital certificate public key.

S58: The user then uploads the re-encrypted encryption private key (A key) and installs this on the encryption key repository. The user or the key manager then deletes the old copy of the encryption private key (A key) from the encryption key repository.

Providing Access to a Document to a New User

As will be appreciated from the example applications of the present technique described above, document security is provided by encrypting that document with the public key of the private key/public key pair of the encryption keys and storing that document on the document repository. The user can then access that document by downloading the encrypted private key of the encryption key pair, decrypting that private key and then downloading the encrypted document to decrypt that document with the decrypted private key. However, the present technique also provides an opportunity for a user to allow access to that document by another user in a secure manner. To this end, the user downloads and decrypts the private key corresponding to the encryption public key with which the document has been encrypted and encrypts a copy of that private key with the public key of a new user's digital certificate. Figure 7 provides a flow diagram illustrating an example of a process in which a new user is provided with access to the private key for accessing an encrypted document, the document having been encrypted with the corresponding public key of the encryption private key public key pair. Figure 7 is summarised as follows:

S60: A user who is issuing access to a document, for example the document originator, downloads from the key repository a copy of the encrypted private key (A key) which is associated with a particular document to which a new user is to be given access.

S62: The issuing user also downloads the new user's digital certificate public key from the public digital certificate repository.

S64: The issuing user then decrypts the encrypted private key (A key) of the encryption key pair using the digital certificate private key for that user which may be stored on the client terminal or in a smart card or a USB token.

S66: The issuing user then re-encrypts the decrypted private key (A key) with the new user's digital certificate public key.

S68: The new user's encrypted copy of the encryption private key (A key) is then uploaded to the key repository. The new user therefore can access the document corresponding to the encryption private key public/key pair because the new user can download the corresponding encrypted private key (A key) with which the user's corresponding public key has been used to encrypt the document and to decrypt the private key using the new user's digital certificate private key so that the document can be decrypted with the user's encryption private key.

Various modifications may be made to the embodiments described above without departing from the scope of the present invention. For example, it will be appreciated that any form of hash algorithm can be used to generate the hash value, and SHA1 algorithm is but one example of an algorithm, which could be used. Also PKCS7 is provided as one example of a signature and any other signature algorithm can be used to generate an appropriate authorisation and validation of a user's activity. The telecommunications network could be an intranet and/or an internet access so that one advantage of the present invention could be secure access to documents via the internet. Another advantage of the present invention could be to secure access to documents via a corporate LAN/WAN.

Application to Electronic Procurement Systems

Embodiments of the present invention may also be incorporated in electronic data or document exchange systems such as electronic procurement systems or electronic sealed bid systems, such as that disclosed in WO2004/091135. For example, electronic tendering is a form of an electronic sealed bidding system used by organisations such as Government agencies and the public sector for procurement of goods, services, and works. In such applications the procuring agency invites tenders, and interested vendors submit sealed bids in response to tenders. The bids may be securely signed and sealed using encryption techniques such as for example Public

Key Infrastructure methods or digital certificates, and may be required to be opened by specified users of the procuring agency only after a particular date and time. Thus in accordance with the present technique, each party to a secure bid is arranged to poses a digital certificate key pair. This is used to access a private key of an encryption key pair stored in a key repository, encrypted with the public key of the digital certificate key pair. Documents created as part of the secure bid process are stored on a document repository, encrypted with the private key of the encryption key pair. Therefore the document management system can provide:

(i) Secure access and control to procuring agencies so that only designated users have access to tender and bid documents.

(ii) The transfer/replacement of access and control rights of a designated user of a procuring agency mid-way through a tendering process can be achieved without compromising or at least reducing a risk to system or individual security, which might otherwise be caused by sharing of passwords or digital certificates. This may be achieved by either decrypting the transferor's encrypted copy of the private key (A key) of the encryption key pairs associated with the tender/bid document using the transferor's certificate private key and re-encrypting it with the transferee's certificate public key, or alternatively if a Key Manager has been appointed in the organisation the Key Manager can download an encrypted private key associated with the tender/bid document, decrypt it with the Key Manager's certificate private key, and re-encrypt it with the certificate public key of the transferee (i.e., the new designated user). The Key Manager can also delete the encrypted private key associated with the tender/bid document of the transferor (i.e., the old designated user) to deny any further access.

(iii) Opening/decryption of tender documents and sealed bids is only executed when all designated users are present/logged-in, which is frequently mandatory in public sector and government procurement. This can be achieved by splitting the private (A key) associated with the encryption key pairs as described above.

CLAIMS

1. A document security management system for securely managing documents or data files for users, the document management system comprising

a document repository providing a facility for storing data files representing the documents,

a key repository for storing a public key of one or more encryption key pairs, each of the encryption key pairs being associated or intended to be associated with one of the documents stored in the document repository, and each document stored in the document repository is encrypted with the public key of the encryption key pair associated with the document, and

a plurality of client terminals operable to retrieve the documents from the document repository for processing by a user, wherein each user is provided with a digital certificate comprising a certificate key pair, and the key repository includes the private key of the encryption key pair encrypted with the public key of the certificate key pair associated with the user, the client terminal being operable with the private key of the certificate key pair, the client terminal being operable

to decrypt the private key of encryption key pair using the private key of the certificate key pair,

to retrieve the encrypted document from the document repository, and

to decrypt the document using the decrypted private key of the encryption key pair to access the document.

2. A document security management system as claimed in Claim 1, wherein the client terminal is operable

to generate a hash value of the document after the document has been created or edited by a user,

to encrypt the hash value with the private key of the private key of the encryption key pair, and

to store the encrypted hash value with the encrypted document on the document server, and the client terminal is operable when retrieving the document from the document server

to decrypt the hash value which has been stored in association with the document,

to recalculate the hash value from the decrypted document retrieved from the document server, and

to verify that the document corresponds with a version of the document in a form when the hash value which has been stored in association with document was produced, by comparing the recalculated hash value with the hash value which was stored on the document server in association with the document.

3. A document security management system as claimed in Claim 1, wherein the client terminal is operable

to generate a digital signature using the user's private key of the certificate key pair, by

calculating a hash value of the document, and

encrypting the hash value calculated from the document with the private key, and

to store the digital signature in association with the encrypted document in the document server, and the client terminal is operable when retrieving the document from the document server

to retrieve the digital signature associated with the document from the document server,

to re-calculate the hash value from the decrypted document,

to extract the hash value from the digital signature by decrypting the encrypted hash value in the signature

to compare the extracted hash with the re-generated hash, and if the re-generated hash is the same as the extracted hash validating the retrieved digital signature as being authentic.

4. A document security management system as claimed in Claim 2 or 3, wherein the digital signature is a detached digital signature generated in accordance with the Public Key Certificate Standard 7.

5. A document security management system as claimed in any preceding Claim, wherein the client terminal is operable to generate a temporal reference indicating a time and/or a date when the document was created and/or edited,

to encrypt the temporal reference with the public key encryption key pair, and

to communicate the encrypted temporal reference to the document repository, the document repository being operable to store the temporal reference with the document in the document repository.

6. A document management security system as claimed in any preceding Claim, wherein the key repository is operable

to store the public key of the one or more encryption key pairs in the key repository,

to encrypt the private key of the one or more encryption key pairs with the public key of the certificate key pair associated with a user, and

to store the encrypted private key of the one or more encryption key pairs on the key repository.

7. A document security management system as claimed in any preceding Claim, wherein the key repository is arranged to store each private key of the one or more encryption key pairs encrypted with a public key of a key manager's certificate key pair.

8. A method of securely managing documents for users, the method comprising

storing data files representing documents on a document repository,

storing a public key of one or more encryption key pairs on a key repository, each of the encryption key pairs being associated with one of the documents stored in

the document repository, and each document stored in the document repository being encrypted with the public key of the encryption key pair associated with the document,

storing and/or retrieving the documents from the document repository for processing by a user, wherein the key repository includes the private key of encryption key pair encrypted with the public key of a digital certificate key pair associated with the user, the method including

decrypting the private key of the encryption key pair using the private key of the certificate key pair,

retrieving the encrypted document from the document repository, and

decrypting the document using the decrypted private key of the first document private key/public key pair.

9. A method as claimed in Claim 8, the method comprising

generating a hash value of the document after the document has been created or edited by a user,

encrypting the hash value with the private key of the first document private key/public key pair,

storing the encrypted hash value with the encrypted document on the document repository,

decrypting the hash value which has been stored in association with the document,

re-calculating the hash value from the decrypted document retrieved from the document repository, and

verifying that the document corresponds with a version of the document in a form when the hash value which has been stored in association with document was produced, by comparing the recalculated hash value with the hash value which was stored on the document repository in association with the document.

10. A method as claimed in Claim 8, the method comprising

generating a digital signature using the user's private key of the certificate key pair, by

calculating a hash value of the document, and

encrypting the hash value calculated from the document with the public key,

storing the digital signature in association with the encrypted document in the document repository,

retrieving the digital signature associated with the document from the document repository,

re-calculating the hash value from the decrypted document,

re-generating the digital signature by encrypting the re-calculated hash value with the user's public key of the second document private key/public key pair, and

comparing the retrieved digital signature with the re-generated digital signature, and if the re-generated digital signature is substantially the same as the re-retrieved digital signature validating the retrieved digital signature as being authentic.

11. A document repository for a document management system operable to manage securely documents for users, the document repository providing a facility for storing data files representing documents, the document repository being operable

to store the data files representing the documents each document stored in the document repository being encrypted with the public key of the first document private key/public key pair associated with the document,

to store in association with each of the documents a hash value generated from the document and a digital signature generated from the hash value and the private key of a second document private key/public key pair provided to a user.

12. A client terminal operable in combination with a key repository and a document repository of a document security management system, the client terminal being operable to store and to retrieve the documents to and from the documentary repository for processing by a user, wherein each user possesses a digital certificate comprising a certificate key pair, and the key repository includes the private key of the encryption key pair encrypted with the public key of the certificate key pair associated with the user, the client terminal being provided by the user with the private key of the certificate key pair, the client terminal being operable

to decrypt the private key of the encryption key pair using the private key of the certificate key pair,

to retrieve the encrypted document from the document repository, and

to decrypt the document using the decrypted private key of the encryption key pair.

13. A client terminal as claimed in Claim 12, wherein the client terminal is operable

to create a data file representing a document,

to encrypt the data file with the public key of the one or more encryption key pairs, and

to store the encrypted data file on the document repository.

14. A key repository operable in combination with a document repository and one or more client terminals to provide a document security management system, the key repository being operable

to store a public key of one or more encryption key pairs, each of the encryption key pairs being associated with one of the documents stored in the document repository, and each document stored in the document repository is encrypted with the public key of the encryption key pair associated with the document, wherein the key repository includes the private key of the encryption key pair encrypted with a public key of a digital certificate key pair associated with the user.

15. A document security management system, a document repository server, a client terminal substantially as herein before described with reference to the accompanying drawings.

16. A method of managing documents substantially as herein before described with reference to the accompanying drawings.

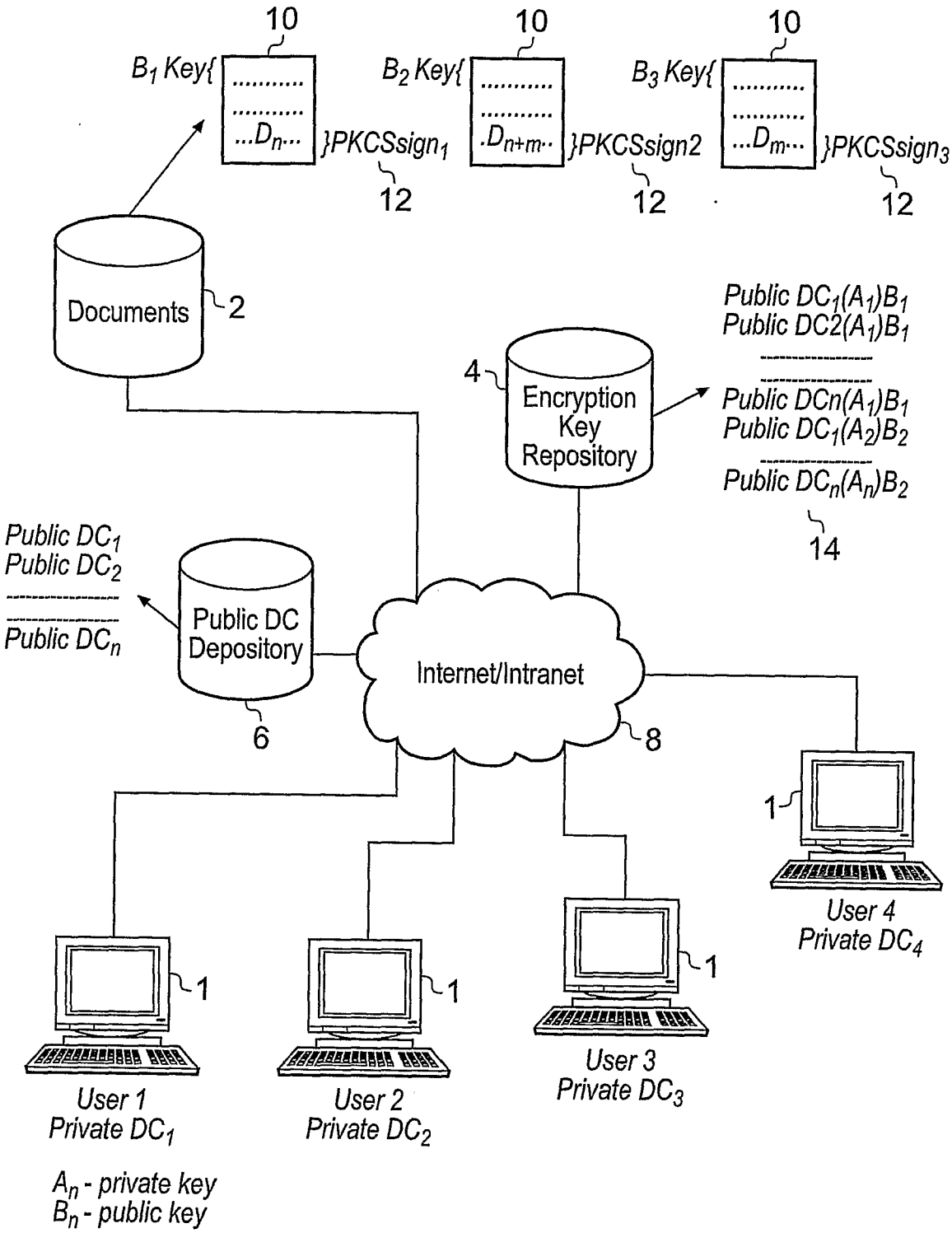

10
10
10
B1 Key{
B2 Key{
B3 Key{
...Dn...
.Dn+m..
...Dm...
}PKCSsign1
}PKCSsign2
}PKCSsign3
12
12
12
Documents
2
4
Encryption Key Repository
Public DC1(A1)B1
Public DC2(A1)B1
Public DCn(A1)B1
Public DC1(A2)B2
Public DCn(An)B2
14
Public DC1
Public DC2
Public DCn
Public DC Depository
6
Internet/Intranet
8
1
1
1
1
User 1
Private DC1
User 2
Private DC2
User 3
Private DC3
User 4
Private DC4
An - private key
Bn - public key

Fig. 1

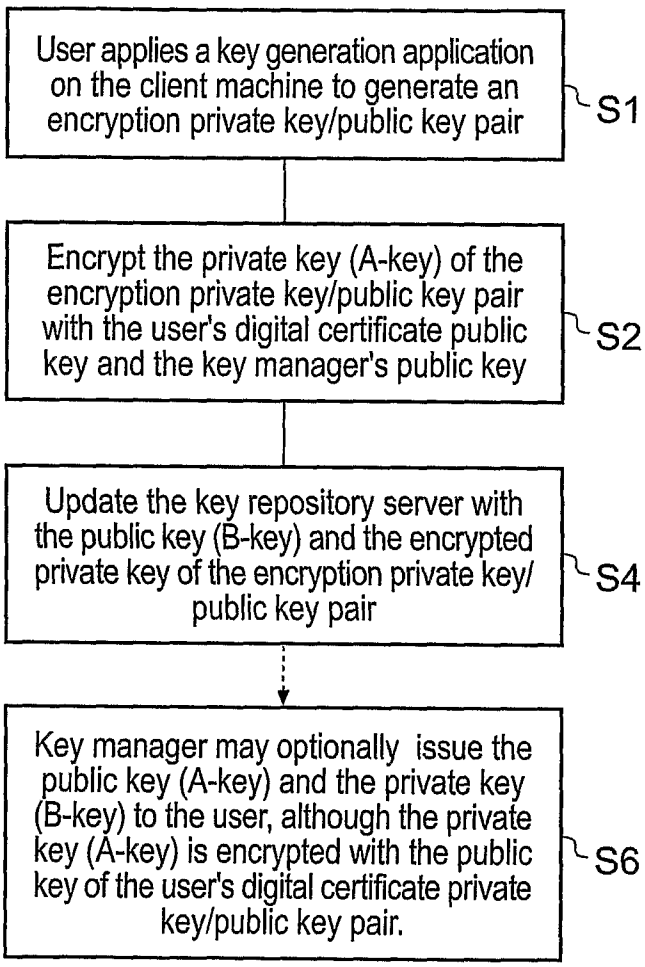

User applies a key generation application on the client machine to generate an encryption private key/public key pair
S1
Encrypt the private key (A-key) of the encryption private key/public key pair with the user's digital certificate public key and the key manager's public key
S2
Update the key repository server with the public key (B-key) and the encrypted private key of the encryption private key/ public key pair
S4
Key manager may optionally issue the public key (A-key) and the private key (B-key) to the user, although the private key (A-key) is encrypted with the public key of the user's digital certificate private key/public key pair.
S6

Fig. 2

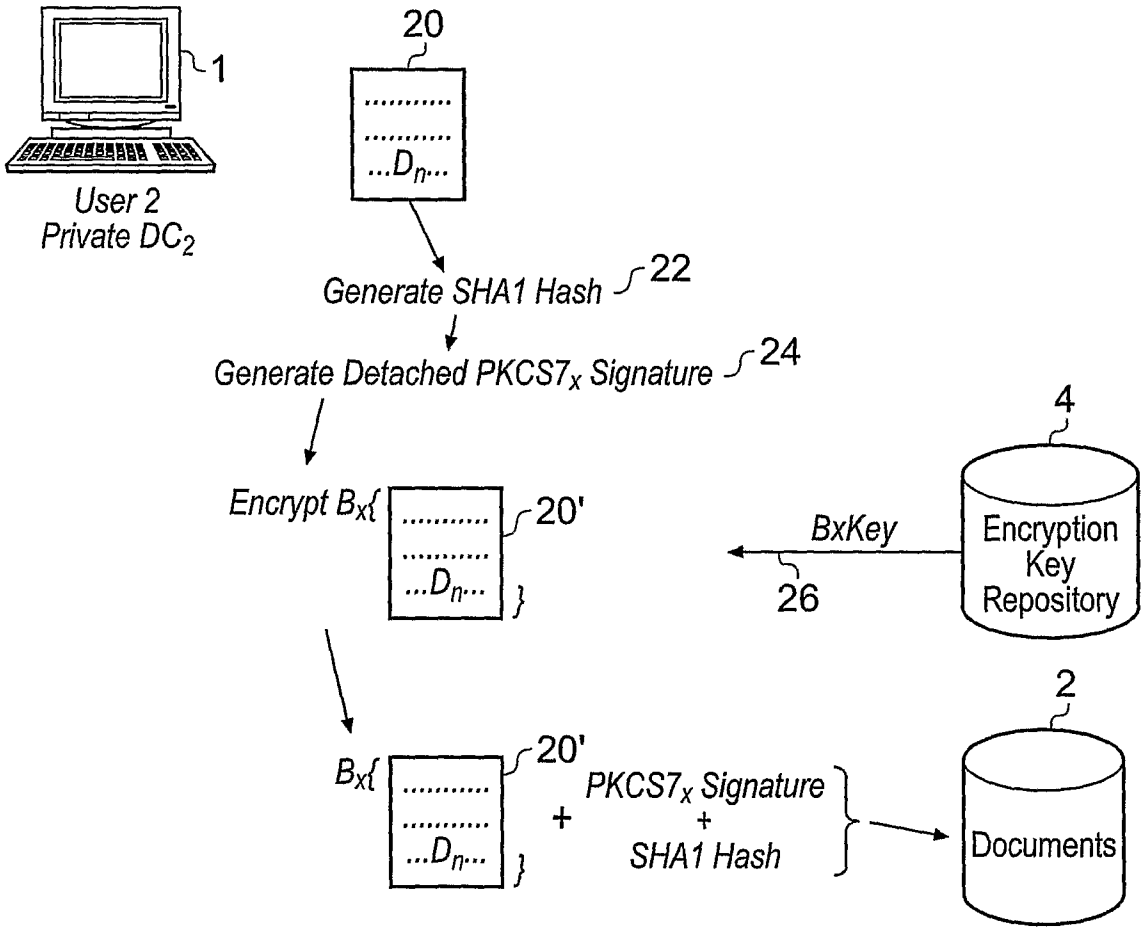

1
User 2
Private DC2
20
.....
.....
...Dn...
Generate SHA1 Hash
22
Generate Detached PKCS7x Signature
24
Encrypt Bx{
.....
.....
...Dn...
}
20'
BxKey
26
4
Encryption
Key
Repository
Bx{
.....
.....
...Dn...
}
20'
+
PKCS7x Signature
+
SHA1 Hash
2
Documents

Fig. 3

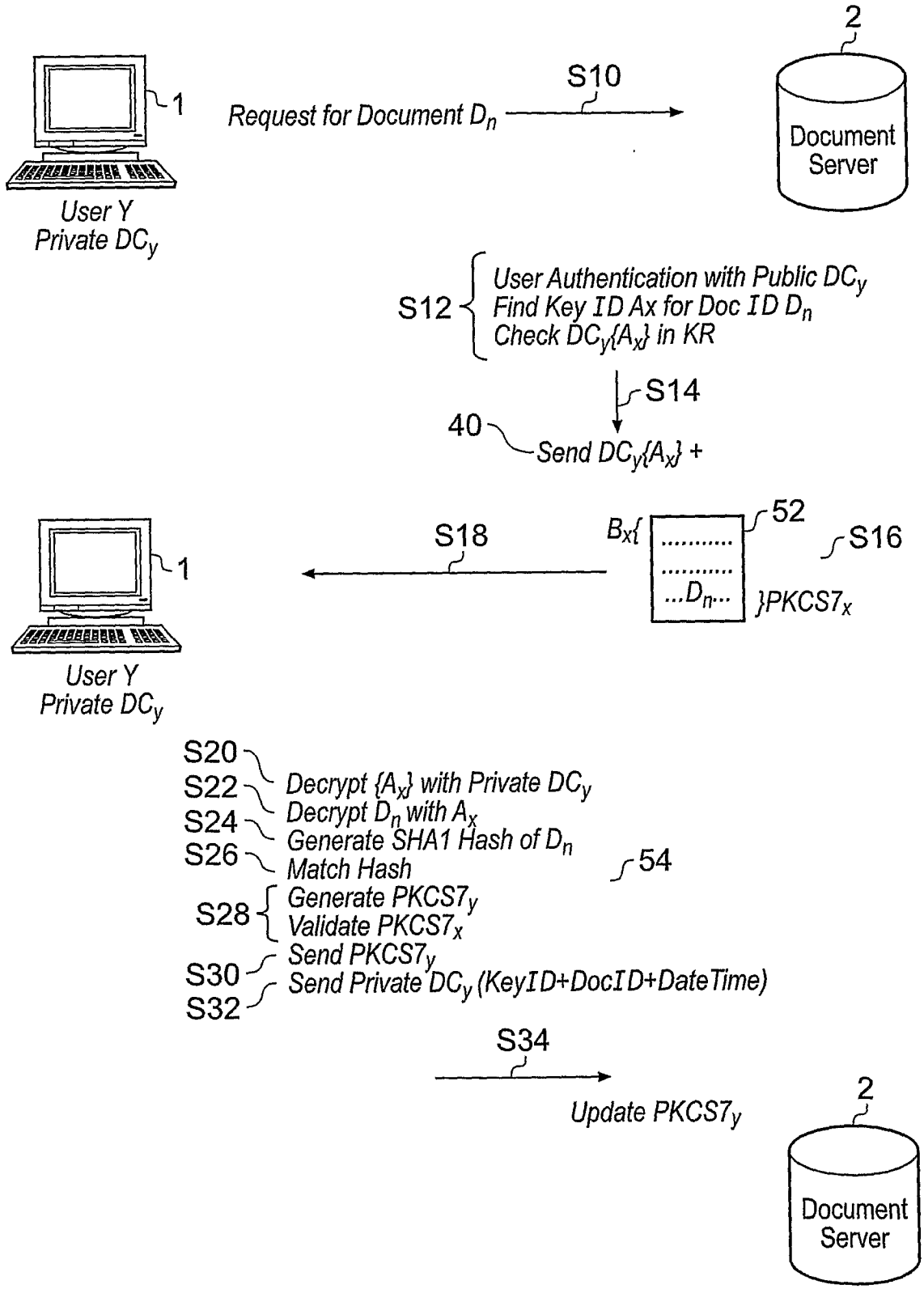

2
1
S10
Request for Document D_n
Document Server
User Y
Private DC_y
S12
User Authentication with Public DC_y
Find Key ID Ax for Doc ID D_n
Check $DC_y\{A_x\}$ in KR
S14
40
Send $DC_y\{A_x\}$ +
52
S16
S18
$B_x\{$
.....
.....
...D_n...
$\}PKCS7_x$
1
User Y
Private DC_y
S20
Decrypt $\{A_x\}$ with Private DC_y
S22
Decrypt D_n with A_x
S24
Generate SHA1 Hash of D_n
S26
Match Hash
54
S28
Generate $PKCS7_y$
Validate $PKCS7_x$
S30
Send $PKCS7_y$
S32
Send Private DC_y (KeyID+DocID+DateTime)
S34
Update $PKCS7_y$
2
Document Server

Fig. 4

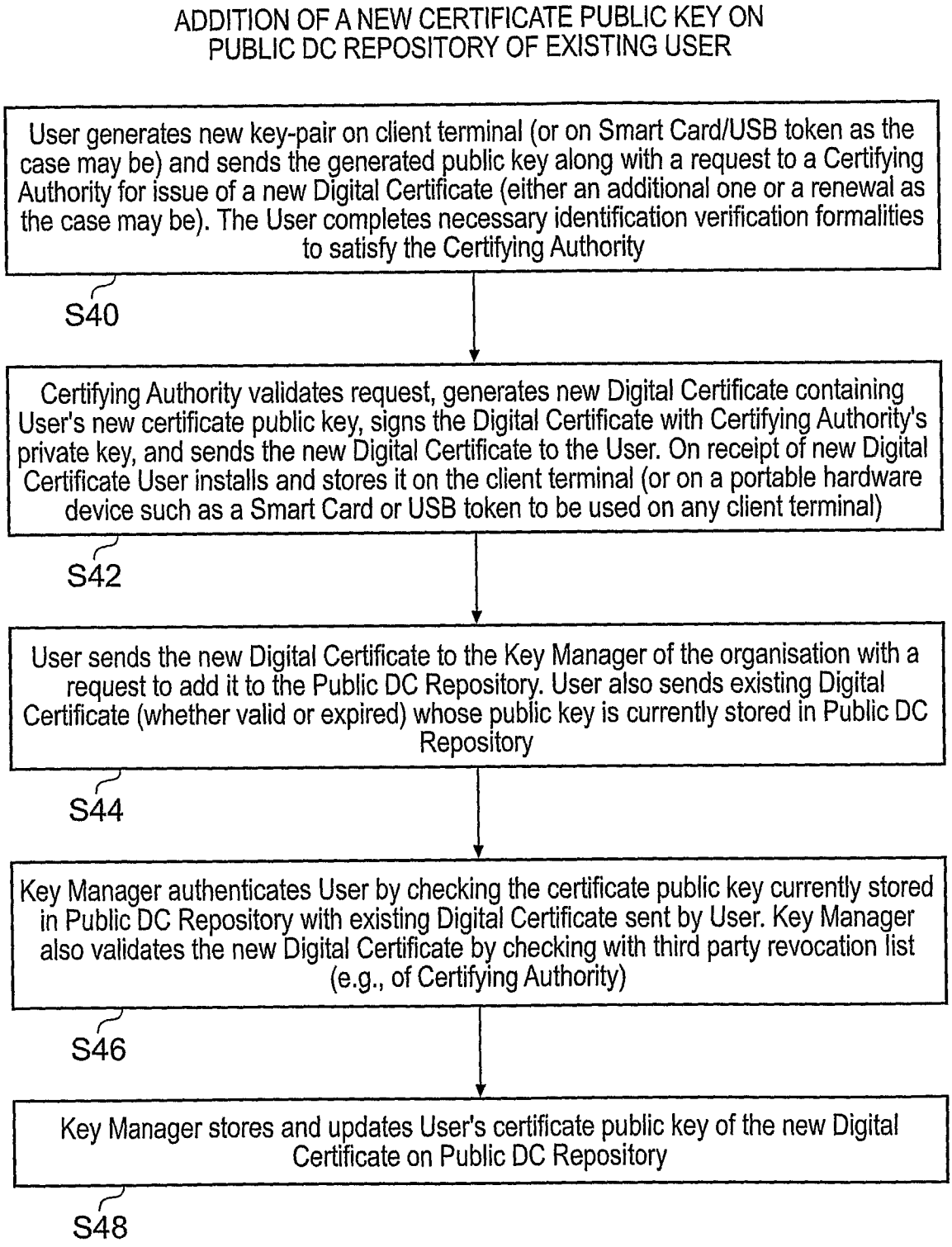

ADDITION OF A NEW CERTIFICATE PUBLIC KEY ON PUBLIC DC REPOSITORY OF EXISTING USER
User generates new key-pair on client terminal (or on Smart Card/USB token as the case may be) and sends the generated public key along with a request to a Certifying Authority for issue of a new Digital Certificate (either an additional one or a renewal as the case may be). The User completes necessary identification verification formalities to satisfy the Certifying Authority
S40
Certifying Authority validates request, generates new Digital Certificate containing User's new certificate public key, signs the Digital Certificate with Certifying Authority's private key, and sends the new Digital Certificate to the User. On receipt of new Digital Certificate User installs and stores it on the client terminal (or on a portable hardware device such as a Smart Card or USB token to be used on any client terminal)
S42
User sends the new Digital Certificate to the Key Manager of the organisation with a request to add it to the Public DC Repository. User also sends existing Digital Certificate (whether valid or expired) whose public key is currently stored in Public DC Repository
S44
Key Manager authenticates User by checking the certificate public key currently stored in Public DC Repository with existing Digital Certificate sent by User. Key Manager also validates the new Digital Certificate by checking with third party revocation list (e.g., of Certifying Authority)
S46
Key Manager stores and updates User's certificate public key of the new Digital Certificate on Public DC Repository
S48

Fig. 5

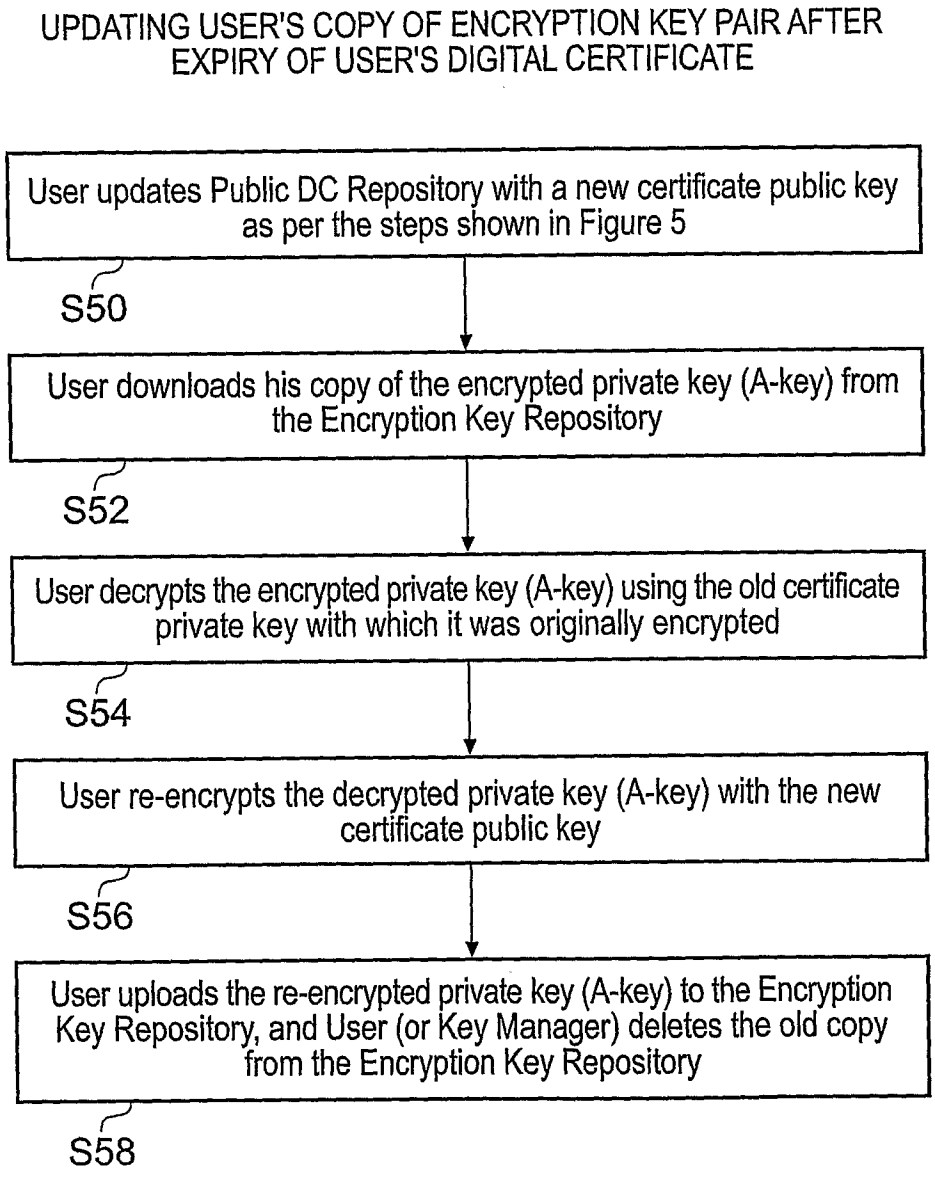

UPDATING USER'S COPY OF ENCRYPTION KEY PAIR AFTER EXPIRY OF USER'S DIGITAL CERTIFICATE
User updates Public DC Repository with a new certificate public key as per the steps shown in Figure 5
S50
User downloads his copy of the encrypted private key (A-key) from the Encryption Key Repository
S52
User decrypts the encrypted private key (A-key) using the old certificate private key with which it was originally encrypted
S54
User re-encrypts the decrypted private key (A-key) with the new certificate public key
S56
User uploads the re-encrypted private key (A-key) to the Encryption Key Repository, and User (or Key Manager) deletes the old copy from the Encryption Key Repository
S58

Fig. 6

ISSUING EXISTING ENCRYPTION KEY PAIRS TO A NEW USER

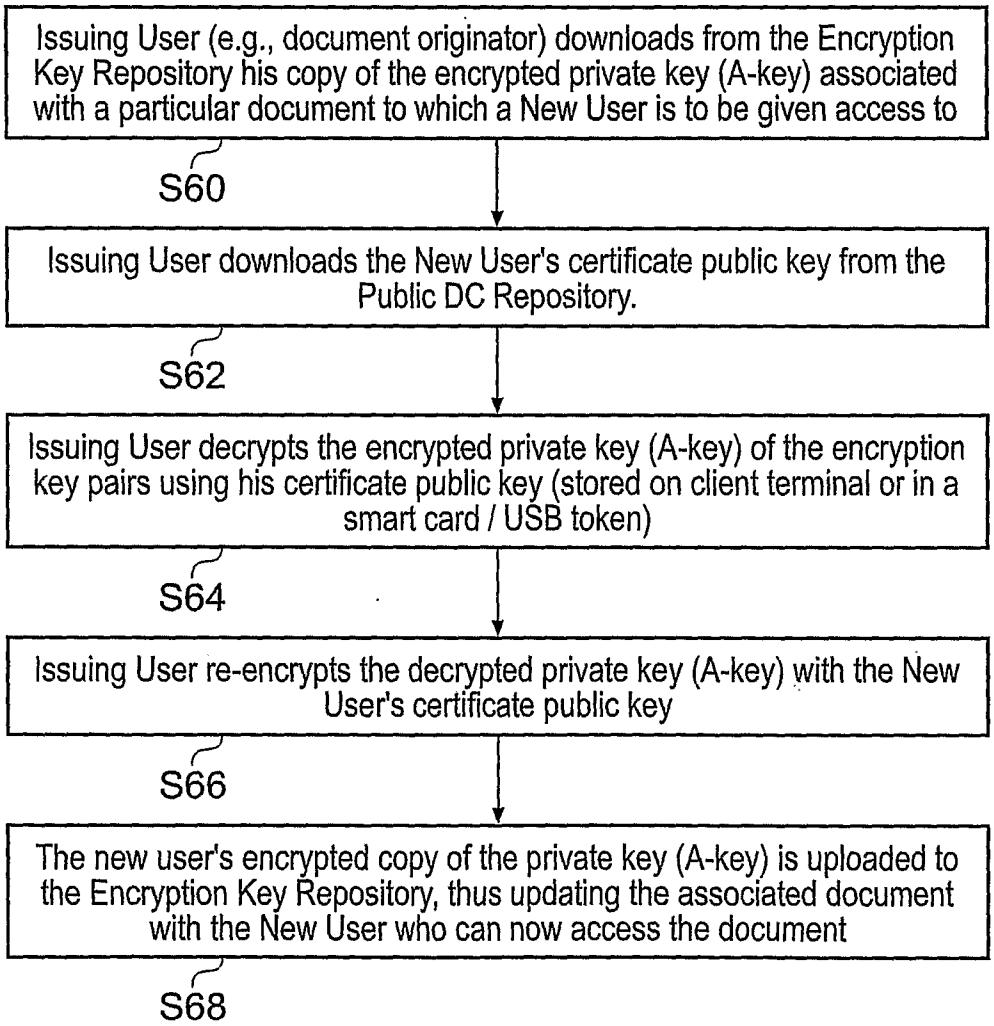


Fig. 7

Box No. VIII (v) DECLARATION: NON-PREJUDICIAL DISCLOSURES OR EXCEPTIONS TO LACK OF NOVELTY

The declaration must conform to the standardized wording provided for in Section 215; see Notes to Boxes Nos. VIII, VIII (i) to (v) (in general) and the specific Notes to Box No. VIII (v). If this Box is not used, this sheet should not be included in the request.

Declaration as to non-prejudicial disclosures or exceptions to lack of novelty (Rules 4.17(v) and 51*bis*.1(a)(v)):

Declaration as to non-prejudicial disclosures or exceptions to lack novelty (Rules 4.17(v) and 51bis.1(a)(v)):

in relation to this international application Jonathan Mark DeVile, Patent Attorney for the Applicants on information provided by Tapan Mehta, Managing Director for the Applicant Company Nextenders (India) Private Limited Company declares that the subject matter claimed in this international application was disclosed as follows:

(i) kind of disclosure (include as applicable):

A disclosure as a result of an abuse in breach of confidence and fiduciary duty, by an e-mail sent on 17 November 2005 to the Executive Director of 3i Infotech Limited by the inventor and Chief Technical Officer Mr Ravindra Shevade. The e-mail included an attachment providing drawings which are substantially the same as Figures 1, 3 and 4 of the present International patent application.

☐ This declaration is continued on the following sheet, "Continuation of Box No. VIII (v)".

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2006/001766

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/24

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)
G06F

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/52473 A (CRITICAL PATH, INC) 19 July 2001 (2001-07-19)	1,3,4, 6-8, 10-14
A	page 5, line 28 - page 6, line 14 page 12, line 22 - page 13, line 22 page 14, line 8 - line 20 page 20, line 32 - page 21, line 4 page 25, line 3 - page 26, line 21	2,5,9
A	WO 00/62220 A (ILUMIN CORPORATION) 19 October 2000 (2000-10-19) figure 2B	1-14
A	EP 0 647 895 A (FISCHER, ADDISON M) 12 April 1995 (1995-04-12) column 1, line 41 - line 53	7

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

"E" earlier 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	Date of mailing of the international search report
6 November 2006	20/11/2006

Name and mailing address of the ISA/	Authorized officer
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	Veillas, Erik

INTERNATIONAL SEARCH REPORT

International application No.
PCT/GB2006/001766

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 15-16
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box II.2

Claims Nos.: 15-16

These claims refer to the description as a whole and to the drawings.

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guideline C-VI, 8.5), should the problems which led to the Article 17(2) declaration be overcome.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2006/001766

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0152473 A	19-07-2001	AU 4359100 A	24-07-2001
		TW 474080 B	21-01-2002
WO 0062220 A	19-10-2000	AU 4460600 A	14-11-2000
		EP 1177517 A1	06-02-2002
EP 0647895 A	12-04-1995	AU 674560 B2	02-01-1997
		AU 5782594 A	13-04-1995
		CA 2120667 A1	05-04-1995
		JP 8171535 A	02-07-1996
		US 5436972 A	25-07-1995
		US 6141423 A	31-10-2000