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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 March 2009 (26.03.2009)

PCT

(10) International Publication Number
WO 2009/036511 A1

(51) International Patent Classification:
*H04L 9/32* (2006.01) *G06F 12/00* (2006.01)

(21) International Application Number:
PCT/AU2008/001392

(22) International Filing Date:
19 September 2008 (19.09.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2007216833 19 September 2007 (19.09.2007) AU
2008901033 3 March 2008 (03.03.2008) AU

(71) Applicant *(for all designated States except US)*: **LOCKSTEP TECHNOLOGIES PTY LTD** [AU/AU]; 11 Minnesota Avenue, Five Dock, New South Wales 2046 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **WILSON, Stephen** [AU/AU]; 11 Minnesota Avenue, Five Dock, New South Wales 2046 (AU).

(74) Agent: **FB RICE & CO**; Level 23, 200 Queen Street, Melbourne, Victoria 3000 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *with international search report*

(54) **Title:** VERIFYING A PERSONAL CHARACTERISTIC OF USERS OF ONLINE RESOURCES

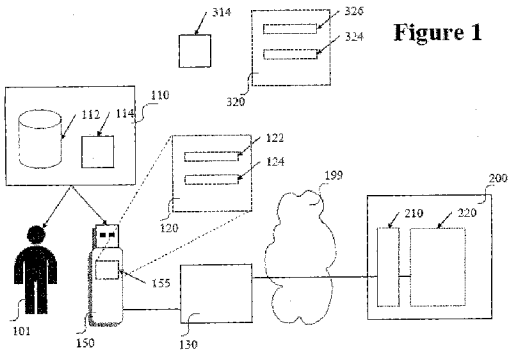



Figure 1

(57) **Abstract:** Access to an electronically accessible resource provided for a defined demographic group is controlled. A cryptographic Private Key is securely stored in a storage device of a user, whether a multi-function storage device or a device dedicated for this purpose. A Public Key Certificate corresponding to the Private Key is also issued to the user. The Public Key Certificate contains data that indicates that the user is a member of the defined demographic group. The Public Key Certificate is signed by or on behalf of a Trusted Third Party trusted to attest to the user being a member of the defined demographic group. An access control system associated with the electronically accessible resource uses the Public Key Certificate to verify that the user is eligible to access the electronically accessible resource by virtue of possessing the demographic characteristic. A Root Certification Authority for broad deployment of the infrastructure is also provided.

WO 2009/036511 A1

**"Verifying a personal characteristic of users of online resources"**

Cross-Reference to Related Applications

The present application claims priority from Australian Provisional Patent Application No 2007216833 filed on 19 September 2007, Australian Provisional Patent Application No 2008901033 filed on 3 March 2008, the contents of which are incorporated herein by reference.

Technical Field

The present invention relates to controlling access to online resources according to personal characteristics such as user age, while allowing preservation of user privacy. In particular the present invention provides for verification of the personal characteristic of the user, without requiring disclosure of the user's identity to the operator of the online resource, and without requiring contemporaneous averment by a third party.

Background of the Invention

The Internet has given rise to a host of innovative new information resources, such as services oriented towards children for purposes including education and entertainment. "Social networking" is an important new type of online service enabled essentially by Internet technologies. In social networking groups of people with common interests or attributes can communicate with one another, share data, undertake discussions, be introduced to like-minded new friends and colleagues, and so on. Typically, access to social networking resources is qualified by some means in order to preserve the collective identity of the group, and protect the privacy of participants. In the case of online resources intended only for children, the most important qualification is the age of the user. Unfortunately, qualifications such as age for participating in social networking services have been difficult to enforce.

Social networking services are increasingly popular among children, who use features such as chat rooms in order to meet and interact with people. Yet various forms of child abuse occur in association with Internet social networking. The traditional difficulty in authenticating strangers on the Internet allows adults to pass themselves

off as children online, and subsequently draw unsuspecting minors into their confidence.

Currently, social networking services for minors have few if any robust defences against adults passing themselves off as children. Qualifying personal details typically must be provided when a new user registers for a given social networking service, yet nothing stops wrongdoers lying about their age.

To protect minors against adults online who might mean them harm, much of the onus has been on educating children to not disclose excessive personal details about themselves, and to remain alert to anomalous behaviours by others online that might indicate that those others might not in fact be children. However these safeguards are imperfect. Children by their nature are not inclined to be reserved or self-limiting in their disclosures, especially when personal information has significant currency in social networking. That is, the usefulness of social networking depends to a large extent on being able to reveal personal details about oneself. Further, child abusers can adopt sophisticated strategies for masquerading as children and thus evade detection for long periods of time.

A technically comparable problem is associated with controlling the access to online resources intended only for adults (generally speaking, persons who have attained the age of majority). Such resources include online gambling, dating and introduction services, "adult" or pornographic content, and other classified content (films, television programs, literature and so on). In Australia for example, new regulations introduced in 2007 require age verification for content delivered over the Internet or to multi-media wireless devices such as mobile telephones when that content has been given a conventional film & television classification of "MA15+" (intended only for a "Mature Audience" over the age of 15) or "R18+" (Restricted to persons over the age of 18).

When verifying the age of users of online resources, whether they are supposed to be children (of the age of minority) or adults (of the age of majority), it is highly desirable

that users be permitted to keep as much as possible of their other identifying information private. That is, an ideal situation is for an online user to be able to assert their exact age or their age group to a service provider without needing to reveal anything else about their identity. Maintaining privacy in children's online social networking is essential for as mentioned, it is wise for children to not disclose excessive personal details. Maintaining privacy in connection with access to adult oriented online resources is equally important: there can be stigma associated with the use of adult oriented sites, and the use of aliases in dating services is common.

Methods for age verification that require users to disclose details such as their full name or their date of birth are therefore unattractive to users wishing to withhold their identity.

One approach to the age verification problem is to have a trusted third party vouch for the age of a first party (the user) at the time when the user is accessing services of a second party (the online service provider). Some approaches to such age verification involve a new type of trusted third party that provides age verification services possibly on a commercial basis, typically by accessing authoritative repositories of age information. When a service provider wishes to confirm the age of a given user, they inquire with the third party as to the person's age. This approach requires the user to provide personal details when registering with the trusted third party, which represents an effort and possible additional expense not normally associated with the use of such resources as online social networking sites. This type of approach also complicates the processes by which the service provider deals with its users, and can involve the disclosure of personal details of the user to the service provider. Moreover, this approach requires a timely response from the third party as user participation is prevented until verification is provided by the third party.

Any discussion of documents, acts, materials, devices, articles or the like which has been included in the present specification is solely for the purpose of providing a context for the present invention. It is not to be taken as an admission that any or all of

these matters form part of the prior art base or were common general knowledge in the field relevant to the present invention as it existed before the priority date of each claim of this application.

Throughout this specification the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated element, integer or step, or group of elements, integers or steps, but not the exclusion of any other element, integer or step, or group of elements, integers or steps.

Summary of the Invention

According to a first aspect the present invention provides a method for controlling access to an electronically accessible resource provided for a defined demographic group, the method comprising:

securely storing in a storage device of a user a cryptographic Private Key;

issuing to the user a Public Key Certificate corresponding to said Private Key, the Public Key Certificate including data that indicates that the user is a member of the defined demographic group, and the Public Key Certificate being signed by or on behalf of a Trusted Third Party trusted to attest to the user being a member of the defined demographic group; and

an access control system associated with the electronically accessible resource using said Public Key Certificate to verify that the user is eligible to access the electronically accessible resource.

According to a second aspect the present invention provides a method for providing a user with demographic verification, the method comprising:

securely storing in a storage device of the user a cryptographic Private Key; and

issuing to the user a Public Key Certificate corresponding to said Private Key, the Public Key Certificate including data that indicates that the user is a member of a defined demographic group, and the Public Key Certificate being signed by or on behalf of a Trusted Third Party trusted to attest to the user being a member of the defined demographic group, wherein the Public Key Certificate is such that an access

control system associated with an electronically accessible resource provided for the defined demographic group can use said Public Key Certificate to verify that the user is eligible to access the electronically accessible resource.

According to a third aspect the present invention provides a method for verifying user eligibility to access an electronically accessible resource provided for a defined demographic group, the method comprising:

a user causing provision of a Public Key Certificate to an access control system associated with the electronically accessible resource; and

the access control system verifying whether the user is eligible to access the electronically accessible resource by determining whether said signed Public Key Certificate includes data indicating that the user is a member of the defined demographic group, and determining whether the Public Key Certificate has been signed by or on behalf of a Trusted Third Party trusted to attest to the user being a member of the defined demographic group.

According to a fourth aspect the present invention provides a storage device securely storing a cryptographic Private Key, and a Public Key Certificate corresponding to said Private Key and including data that indicates that the user is a member of a defined demographic group, and the Public Key Certificate being signed by or on behalf of a Trusted Third Party trusted to attest to the user being a member of the defined demographic group.

According to a fifth aspect the present invention provides a computer program element comprising computer program code means to make a computer execute a procedure for controlling access to an electronically accessible resource, the computer program element comprising:

computer program code means for obtaining from a user a Public Key Certificate; and

computer program code means for verifying whether the user is eligible to access the electronically accessible resource by determining whether said signed Public

Key Certificate includes data indicating that the user is a member of the defined demographic group, and determining whether the Public Key Certificate has been signed by or on behalf of a Trusted Third Party trusted to attest to the user being a member of the defined demographic group.

The present invention thus provides for the Public Key Certificate to verify that the user is a member of a particular demographic group, such as being within a particular age group, without requiring that any other personal details about the user such as their identity be revealed. Thus the present invention provides a secure means by which to establish the user's authorisation to access the resource in question, without requiring authentication of the user's identity.

Such a Public Key Certificate in combination with a cryptographic storage device and Private Key provides a particularly strong mechanism for differentiating members of the relevant demographic group, for example for differentiating children from adults. Use of a cryptographic storage device and public key infrastructure provides resistance to copying or counterfeiting as might be attempted by an adult that would masquerade as a child. Providing the user with a private key gives the user a means to demonstrate that the Public Key Certificate is in fact associated with that individual, so as to prevent copies of the Certificate from being made and used by others.

The present invention also represents a form of two factor authentication and is therefore more resistant to theft and abuse than are traditional single factor authentication methods such as secret passwords used to control access to social networking services. If a child loses their cryptographic storage device then it is relatively easy to be alerted to that fact and prevent others from inappropriately using the device by cancelling the Certificate, and relatively easy to replace together with a new Public Key Certificate.

The Certificate may be issued to the user by being stored in connection with a storage device which is required to be kept in the possession of the user for other purposes, for

example a driver's license, student concession card, membership card, a telephone or a personal digital assistant (PDA). Loss or theft of such a device is likely to be promptly reported by the user allowing cancellation of the Public Key Certificate to prevent others from using a stolen device to access the electronically accessible resource. The storage device could be a magnetic stripe card, a USB storage device, a smart card, a subscriber identity module (SIM) card, a random access memory or read only memory of a telephone or PDA, or other suitable device.

Preferably, the trusted third party is a body that, due to existing responsibilities, has the knowledge required to attest to the user's demographic status of interest. For example, where the demographic group is children of school age, preferred embodiments of the present invention provide for the trusted third party to be an institution such as a government department of education and/or a body responsible for issuing student concession cards, for example. Such embodiments ease implementation of the system of the present invention, by recognising that a typical routine function of such bodies is to produce and issue to school children public transport concession cards and the like, which in effect vouch for the fact that the card holder is a school age child. The present invention provides the means for that existing trusted third party to provide verification of age to the child in digital cryptographic form for use online, with the additional benefit in some embodiments of being able to de-identify the child in the online environment. Moreover, such embodiments of the present invention are further advantageous in providing a "push" distribution model for certificates, where the trusted third party acts as a 'source of truth' and feeds data to a Certificate Authority for the automatic production of certificates, avoiding the need for individuals to 'pull' down certificates by application. Thus, if for example a school student is eligible for a proof-of-age certificate, then the Certificate can be produced without requiring the student to undergo an arduous application process and without engaging any new authorities or service providers.

Embodiments of the invention preferably provide for one or more Root Certification Authorities each being trusted to attest that particular institutions are authorised to aver

demographic characteristics of the user. Such embodiments of the invention provide for cross-jurisdictional implementation of the present invention, in providing for verification of a user's demographic characteristic when accessing an electronic resource based in a jurisdiction different to the jurisdiction in which the user is located. That is, such embodiments recognise that the electronically accessible resource may be in a different country or different jurisdiction to the user, and recognise that the provider of the electronically accessible resource may not have first hand knowledge of whether the institution is legitimately authorised to aver the demographic characteristics of the user.

By providing a Root Certification Authority responsible for maintaining a list of appropriately authorised bodies in different jurisdictions, such embodiments of the invention enable access control to the electronically accessible resource to be effected in an automated and rapid manner, by ensuring that the Public Key Certificate presented by the user and issued by an institution properly chains back to the Root Certification Authority. To establish such Root Certification requires the simple step of the Root Certification Authority issuing Public Key Certificates to one or more corresponding trusted third party Certification Authorities in each jurisdiction.

In cross-jurisdictional embodiments of the invention, the Root Certification Authority preferably further attests as to which particular demographic characteristic(s) each institution is authorised to aver. For example, the Root Certification Authority may attest that a government department of education is authorised to aver that children are minors. In such embodiments, the Root Certification Authority preferably maintains a code numbering schema, electronic directory service or similar means to identify which particular demographic characteristic is vouched for by the institution through the Public Key Certificates issued to individuals. A suitable code numbering schema could for example be constructed using X.500 standard Object Identifiers (OIDs) administered by the Root Certification Authority.

The demographic group may be defined by any suitable demographic characteristic(s), such as: age; gender; race; religion; sexual orientation; income; special interests; membership or affiliation with a society, social networking site, online gaming community or virtual world; geographic or virtual location; nationality; residential jurisdiction; disease status; and/or entitlement to social security benefits or old age benefits.

The storage device may be issued to the user by the trusted third party and may serve other purposes such as being a transport concession card for a student, or a driver's license for an adult. Alternatively, the storage device may be incorporated into another electronic device such as a portable digital assistance (PDA), mobile telephone handset, or personal computer. Embodiments utilising a portable device provide benefits including resistance to replay attack, identity theft, counterfeiting and the like, provide ease of use, and provide improved confidence in the user acting consensually in the use of the Private Key since it is unlikely that a physical device is used inadvertently. In embodiments of the invention in which a Private Key is stored in a storage device of the user, the Private Key and the Public Key Certificate are preferably stored in the same device, and may both be stored in a single storage means of the device. The storage device may comprise any suitable storage device such as a smartcard, a cryptographic USB key, a regular USB key, a mobile telephone Subscriber Identification Module (SIM) card, other memory of a mobile telephone or Personal Data Assistant, tamper resistant storage, or a hardware security module such as a Trusted Platform Module.

Preferably, the Public Key Certificate is anonymous in so far as the certificate contents do not include any personally identifiable information, and reveal only the fact averred by the Trusted Third Party that the user belongs to a certain demographic group such as being of a certain age. However in some embodiments it may be desirable for other purposes to include within the Public Key Certificate or within the storage device information identifying the user. The storage device may be equipped with visual indicia identifying the user, or alternatively may carry no visual means to identify the

user. The storage device may store one or more other Private Keys or Public Key Certificates for other purposes, for example to establish the identity of the user in other applications.

In preferred embodiments of the present invention, the cryptographic storage device includes a built-in function for generating Public Key / Private Key pairs, such that following generation the Private Key never leaves the confines of the storage device. Such embodiments are advantageous in making it highly difficult for the storage device and its contents to be copied or counterfeited by illegitimate users.

In some embodiments of the present invention, when applied to the demographic group of children of minority age the storage device is preferably a tamper resistant cryptographic USB key. Such an embodiment is advantageous as being relatively easy to use by children, and is further advantageous in exploiting that USB devices are inexpensive, in widespread use, and are compatible with the great majority of contemporary personal computers and thus require no special reader device in order to be interfaced to a personal computer.

In embodiments of the invention, to authenticate that the user is properly associated with the Public Key Certificate, any suitable technique may be applied, for example the Private Key of the user may be used to produce a cryptogram from a challenge in a challenge-response protocol. Additionally or alternatively the Private Key of the user may be used to produce a cryptogram from a transactional data object where said cryptogram may be verifiable by means of the Public Key Certificate corresponding to said Private Key.

Brief Description of the Drawings

An example of the invention will now be described with reference to the accompanying drawings, in which:

Figure 1 illustrates a system for issuing to children cryptographic USB keys including Public Key Certificates that verify the age of those children when accessing online resources; and

Figure 2 illustrates a general-purpose computing device that may be used in an exemplary system for implementing the invention;

Description of the Preferred Embodiments

The presently described embodiment of the present invention recognises the specific relationship that children as students can have with institutions such as Departments of Education, which have established processes for issuing to children documents or cards that aver eligibility for such concessions as discounted public transport fares. In this embodiment of the present invention, a Department of Education acts as a Trusted Third Party that issues Public Key Certificates that verify the age of each child receiving such a certificate. Any provider of online resources intended only for children can design their access control systems to use such Public Key Certificates to distinguish between children verified as such by the Department of Education, and other illegitimate users such as adults.

With reference to Figure 1, a Department of Education 110 maintains a database 112 of school age children. The Department of Education 110 issues to a child 101 listed in the database 112 a cryptographic USB key 150. The cryptographic USB key 150 includes a processor chip 155. During the process of personalising and issuing the cryptographic USB key 150, the processor chip 155 generates a Public Key – Private Key pair. A Public Key Certificate 120 corresponding to said Public Key – Private Key pair is created and signed by a Certification Authority 114 operated by the Department of Education 110. In alternative embodiments the Certification Authority 114 may be a separate party engaged by the Department of Education for this purpose. The Public Key Certificate 120 includes a data item 122 that attests that the child 101 is of school age. The Public Key Certificate 120 also includes a digital signature 124 of the Department of Education 110. The Public Key Certificate 120 is anonymous in that

the identity of the child 101 is not included in the Public Key Certificate 120, in this embodiment.

Subsequently, child 101 uses computer 130 to access via the Internet 199 online resources 220 provided by service provider 200 and intended only for children. The child 101 connects the cryptographic USB key 150 to a personal computer 130 as part of the access control procedure. An access control module 210 associated with the online resources 220 operates so as to distinguish legitimate users such as child 101 from illegitimate users such as adults. The access control module 210 effects verification by examining the Public Key Certificate 120, checking that the digital signature 124 corresponds to the Department of Education 110, and checking that the data item 122 does indicate that the holder of the Public Key Certificate 120 (namely the child 101) is of school age. If said checks are satisfied then the access control module 210 grants child 101 access to the online resources 220.

In this embodiment, the Certification Authority 114 is itself certified by a Root Certification Authority 314 which issues CA Public Key Certificate 320 containing a data item 326 that attests that the Certification Authority 114 is recognised as being authoritative over the particular demographic characteristic in question, in this case the fact that the child 101 is of school age. The CA Public Key Certificate 320 also includes a digital signature 324 of the Root Certification Authority 314. This arrangement thus effects an international or otherwise cross-jurisdictional mechanism for endorsing Certification Authority 114 so that the legitimacy of their verification of age of student 101 may be automatically verified by the service provider 200 even where the Certification Authority 114 is unknown to the service provider 200.

This cross-jurisdictional ability of this embodiment recognises that in respective jurisdictions there could be one or more bodies that are authoritative in vouching for certain demographic characteristics. For instance, in addition to Department of Education 110 acting as an authoritative body in vouching for child 101 being of school age, a driver licensing bureau might act as an authoritative body in vouching for

individuals being of the age of majority. The infrastructure provided by this embodiment, specifically Root Certification Authority 314, enables the standing of such deemed authoritative bodies to be rapidly determined by a secure automated process even across jurisdictional borders.

For authorities to be certified by the Root Certification Authority 314, a formal approval process is implemented. For example where the authority is a driver license authority, the approval process takes advantage of existing international arrangements by which driver licence authorities and therefore driver licences are recognised across jurisdictions.

Therefore, in this embodiment any service provider 200 anywhere in the world can confirm whether a given individual 101 is of school age, no matter where that individual resides. This is because the service provider 200 can check if the person's Public Key Certificate 120 firstly chains back to the Root Certification Authority 314, and secondly that Public Key Certificate 120 contains a code number indicating that the Public Key Certificate issuer 114 is deemed by the Root Certification Authority 314 to be authoritative as to the demographic characteristic of being of school age.

The cross jurisdictional infrastructure provided by this embodiment scales readily. Once the Root Certification Authority 314 is established and its Root Public Key promulgated across all social networking sites such as child social networking site 220, new Certification Authorities 114 can be joined to the scheme at any time, to provide age verification for example, or verification of any other demographic characteristic, again without requiring identification of users.

Thus, service provider 200 is able to gain additional confirmation of the authority of the Department of Education 110 by verifying also that the Public Key Certificate 120 correctly chains cryptographically to CA Public Key Certificate 320 signed by the Root Certification Authority 314. If the Public Key Certificate 120 does correctly chain cryptographically to CA Public Key Certificate 320 then service provider 200 can infer

that the Certification Authority 114 is a recognised member of the inter-jurisdictional set of authoritative bodies able to vouch for demographic characteristics. If the data item 326 further indicates that the Certification Authority 114 has been certified by the Root Certification Authority 314 as being authoritative over the demographic property of being of school age, then the service provider 200 gains additional confirmation of the authority of the Department of Education 110.

This embodiment thus maintains the privacy of child 101 by not requiring the child at any time to provide their actual name or any other identifying details to the social networking service 220. Because the child's age is attested to by the department of education 110, nor does the child need to divulge their name or personal details to third parties. Even in alternative embodiments where the certification authority 114 is a separate party to the department of education 110, that authority 114 does not receive any details identifying the child in their task of producing the certificate 120.

This embodiment thus takes advantage of knowledge that an existing trusted authority, namely department of education 110, already has about the age of the child 101, and further ensures that only the pertinent personal quality is revealed, in that the child is of the age of minority. This embodiment thus avoids introducing or imposing additional parties into the relationship between the service provider 200 and the user 101, providing a verification model which is simple, less risky, cheaper to implement, and lower cost to operate.

Moreover, providing child 101 with a Public Key Certificate issued by the CA 114, this embodiment enables verification to be performed substantially offline. This is because the face-validity of the child's certificate 120 is evident to the service provider 200 without the provider 200 having to make any online inquiries at all, provided they have a trusted copy of the PKI root key. The currency of the child's age verification certificate 120 might need to be checked in real time by provider 200, to ensure that it has not been revoked, however such a real time check can be done with relatively high

performance and low bandwidth requirements using the industry standard OCSP protocol supported by all commercial CAs.

Some portions of this detailed description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

As such, it will be understood that such acts and operations, which are at times referred to as being computer-executed, include the manipulation by the processing unit of the computer of electrical signals representing data in a structured form. This manipulation transforms the data or maintains it at locations in the memory system of the computer, which reconfigures or otherwise alters the operation of the computer in a manner well understood by those skilled in the art. The data structures where data is maintained are physical locations of the memory that have particular properties defined by the format of the data. However, while the invention is described in the foregoing context, it is not meant to be limiting as those of skill in the art will appreciate that various of the acts and operations described may also be implemented in hardware.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the description, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying"

or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The present invention also relates to apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may comprise a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. While noting that some embodiments of the invention require cryptographic functionality and/or tamper-resistant hardware, in the main various general purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will appear from the description. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein.

A machine-readable medium includes any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer). For example, a machine-readable medium includes read only memory ("ROM"); random access memory ("RAM"); magnetic disk storage media; optical storage media; flash memory

devices; electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.); etc.

Turning to Figure 2, the invention is illustrated as being implemented in a suitable computing environment. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by a personal computer. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Moreover, those skilled in the art will appreciate that the invention may be practiced with other computer system configurations, including hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

In Figure 2 a general purpose computing device is shown in the form of a conventional personal computer 20, including a processing unit 21, a system memory 22, and a system bus 23 that couples various system components including the system memory to the processing unit 21. The system bus 23 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory includes read only memory (ROM) 24 and random access memory (RAM) 25. A basic input/output system (BIOS) 26, containing the basic routines that help to transfer information between elements within the personal computer 20, such as during start-up, is stored in ROM 24. The personal computer 20 further includes a hard disk drive 27 for reading from and writing to a hard disk 60, a magnetic disk drive 28 for reading from or writing to a removable magnetic disk 29, and an optical disk drive 30 for reading from or writing to a removable optical disk 31 such as a CD ROM or other optical media.

The hard disk drive 27, magnetic disk drive 28, and optical disk drive 30 are connected to the system bus 23 by a hard disk drive interface 32, a magnetic disk drive interface 33, and an optical disk drive interface 34, respectively. The drives and their associated computer-readable media provide nonvolatile storage of computer readable instructions, data structures, program modules and other data for the personal computer 20. Although the exemplary environment shown employs a hard disk 60, a removable magnetic disk 29, and a removable optical disk 31, it will be appreciated by those skilled in the art that other types of computer readable media which can store data that is accessible by a computer, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, random access memories, read only memories, storage area networks, and the like may also be used in the exemplary operating environment.

A number of program modules may be stored on the hard disk 60, magnetic disk 29, optical disk 31, ROM 24 or RAM 25, including an operating system 35, one or more applications programs 36, other program modules 37, and program data 38. A user may enter commands and information into the personal computer 20 through input devices such as a keyboard 40 and a pointing device 42. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 21 through a serial port interface 46 that is coupled to the system bus, but may be connected by other interfaces, such as a parallel port, game port or a universal serial bus (USB) or a network interface card. A monitor 47 or other type of display device is also connected to the system bus 23 via an interface, such as a video adapter 48. In addition to the monitor, personal computers typically include other peripheral output devices, not shown, such as speakers and printers.

The personal computer 20 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 49. The remote computer 49 may be another personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of

the elements described above relative to the personal computer 20, although only a memory storage device 50 has been illustrated. The logical connections depicted include a local area network (LAN) 51 and a wide area network (WAN) 52. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and, inter alia, the Internet.

When used in a LAN networking environment, the personal computer 20 is connected to the local network 51 through a network interface or adapter 53. When used in a WAN networking environment, the personal computer 20 typically includes a modem 54 or other means for establishing communications over the WAN 52. The modem 54, which may be internal or external, is connected to the system bus 23 via the serial port interface 46. In a networked environment, program modules depicted relative to the personal computer 20, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as described in the specific embodiments disclosed herein, without departing from the spirit or scope of the invention as broadly described. For example, while the described embodiment uses cryptographic USB keys, alternate embodiments may provide an alternative means for securely storing Private Keys associated with Public Key Certificates that verify the age of the user, such alternative means including without limitation smartcards, mobile telephone Subscriber Identification Modules, hardware security modules, and "Trusted Platform Modules".

Further, it will be appreciated by persons skilled in the art of Public Key Infrastructure that there are numerous methods and processes available for generating Public Key – Private Key pairs, generating Public Key Certificates, and personalising and issuing

cryptographic storage devices, and any suitable such method may be adopted in implementing the present invention.

While the embodiment described herein involves cryptographic storage devices and Public Key Certificates being issued by an institution, alternative embodiments can make use of outsourced managed service providers that issue storage devices and Public Key Certificates on behalf of the institution, under contract to the institution.

Further, while the present embodiment relates to verifying the age of users of online resources intended only for children, the present invention is applicable to enforcing other types of access control rules for online resources. Such other rules include without limitation verifying that the user has reached the age of majority, as may be attested to by a driver's license regulator or other suitable trusted body. Such verification of age of majority may be employed by social networking sites intended for adults only and/or sites providing classified content, adult content or gambling content, whether delivered via the Internet to personal computers and the like or via multimedia services to mobile telephones or other wireless devices.

Alternatively the present invention may be employed in verifying that the user attends a certain school, as may be attested to by that school or by a government department of education.

In other embodiments the demographic grouping may be by disease status, for example to attest to the user being free of sexually communicable diseases, as may be attested to by a certified health professional for example.

The demographic group may be membership of a romantic dating community, whereby the user's membership of the community is attested to by a community registrar. The demographic group may be membership of an online virtual world community or an online game such as a massively multiplayer online role playing game, whereby the user's membership of the community is attested to by a community registrar. In

embodiments where community membership is verified, existing members of the community may be permitted to introduce new members by signing the new member's application using their Private Key and Public Key Certificate in order to effect an introduction.

The demographic group may be social security or old age benefit recipients, as may be attested to by a social security agency.

Still further, while the preferred embodiment has been described with reference to a personal computer for accessing online resources, it is to be appreciated that any computing device with network connectivity may be used in implementing the present invention. For example the computing device may comprise a suitably configured "multimedia" or 3G mobile telephone.

In a particular instance, this invention allows differentiation between children and adults in connection to controlling access to online resources intended only for children. In another instance, this invention allows differentiation of users in connection with online resources intended only for adults.

In one variation, a Certificate may be relied upon to verify that the user is a member of a particular demographic group, such as being within a particular age group, without requiring that any other personal details about the user such as their identity be revealed. This affords a means by which to establish the user's authorisation to access the resource in question, without requiring authentication of the user's identity nor use of a private key.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS:

1. A method for controlling access to an electronically accessible resource provided for a defined demographic group, the method comprising:

securely storing in a storage device of a user a cryptographic Private Key;

issuing to the user a Public Key Certificate corresponding to said Private Key, the Public Key Certificate including data that indicates that the user is a member of the defined demographic group, and the Public Key Certificate being signed by or on behalf of a Trusted Third Party trusted to attest to the user being a member of the defined demographic group; and

an access control system associated with the electronically accessible resource using said Public Key Certificate to verify that the user is eligible to access the electronically accessible resource.

2. The method of claim 1 wherein the issuing is performed by or on behalf of the trusted third party and wherein the trusted third party is a body that, due to existing responsibilities, has the knowledge required to attest to the user's demographic status of interest.

3. The method of claim 1 or claim 2 wherein using said Public Key Certificate to verify that the user is eligible to access the electronically accessible resource comprises determining whether the Public Key Certificate chains back to a Root Certification Authority trusted by the access control system.

4. The method of claim 3 further comprising determining whether the Root Certification Authority avers that the Trusted Third Party is trusted to attest to demographic characteristics of the user.

5. The method of claim 4 further comprising accessing a code numbering schema maintained by the Root Certification Authority to identify which particular demographic characteristic is vouched for by the Trusted Third Party through the Public Key Certificate.

6. The method of any one of claims 1 to 5 wherein the demographic characteristic comprises at least one of: age; gender; race; religion; sexual orientation; income; special interests; membership or affiliation with a society, social networking site, online gaming community or virtual world; geographic or virtual location; nationality;

residential jurisdiction; disease status; and entitlement to social security benefits or old age benefits.

7. The method of any one of claims 1 to 6 wherein the Public Key Certificate is anonymous in so far as the certificate contents do not include any personally identifiable information beyond the demographic characteristic averred by the Trusted Third Party.

8. The method of any one of claims 1 to 7 further comprising the access control system authenticating that the user is properly associated with the Public Key Certificate.

9. The method of claim 8 wherein the authenticating comprises the Private Key of the user producing a cryptogram from a challenge in a challenge-response protocol, whereby said cryptogram is verifiable by means of the Public Key Certificate corresponding to said Private Key.

10. The method of claim 8 or claim 9 wherein the authenticating comprises the Private Key of the user producing a cryptogram from a transactional data object, whereby said cryptogram is verifiable by means of the Public Key Certificate corresponding to said Private Key.

11. A method for providing a user with demographic verification, the method comprising:

securely storing in a storage device of the user a cryptographic Private Key; and

issuing to the user a Public Key Certificate corresponding to said Private Key, the Public Key Certificate including data that indicates that the user is a member of a defined demographic group, and the Public Key Certificate being signed by or on behalf of a Trusted Third Party trusted to attest to the user being a member of the defined demographic group, wherein the Public Key Certificate is such that an access control system associated with an electronically accessible resource provided for the defined demographic group can use said Public Key Certificate to verify that the user is eligible to access the electronically accessible resource.

12. A method for verifying user eligibility to access an electronically accessible resource provided for a defined demographic group, the method comprising:

a user causing provision of a Public Key Certificate to an access control system associated with the electronically accessible resource; and

the access control system verifying whether the user is eligible to access the electronically accessible resource by determining whether said signed Public Key Certificate includes data indicating that the user is a member of the defined demographic group, and determining whether the Public Key Certificate has been signed by or on behalf of a Trusted Third Party trusted to attest to the user being a member of the defined demographic group.

13. A storage device securely storing a cryptographic Private Key, and a Public Key Certificate corresponding to said Private Key, the Public Key Certificate including data that indicates that the user is a member of a defined demographic group, and the Public Key Certificate being signed by or on behalf of a Trusted Third Party trusted to attest to the user being a member of the defined demographic group.

14. The storage device of claim 13 wherein the storage device is kept in the possession of the user for other purposes, being at least one of a driver's license, student concession card, membership card, a telephone or a personal digital assistant (PDA).

15. The storage device of claim 13 or claim 14, the storage device comprising at least one of: a magnetic stripe card, a USB storage device, a cryptographic USB storage device, a smart card, a tamper resistant storage, a subscriber identity module (SIM) card, a hardware security module and a random access memory or read only memory of a telephone or PDA.

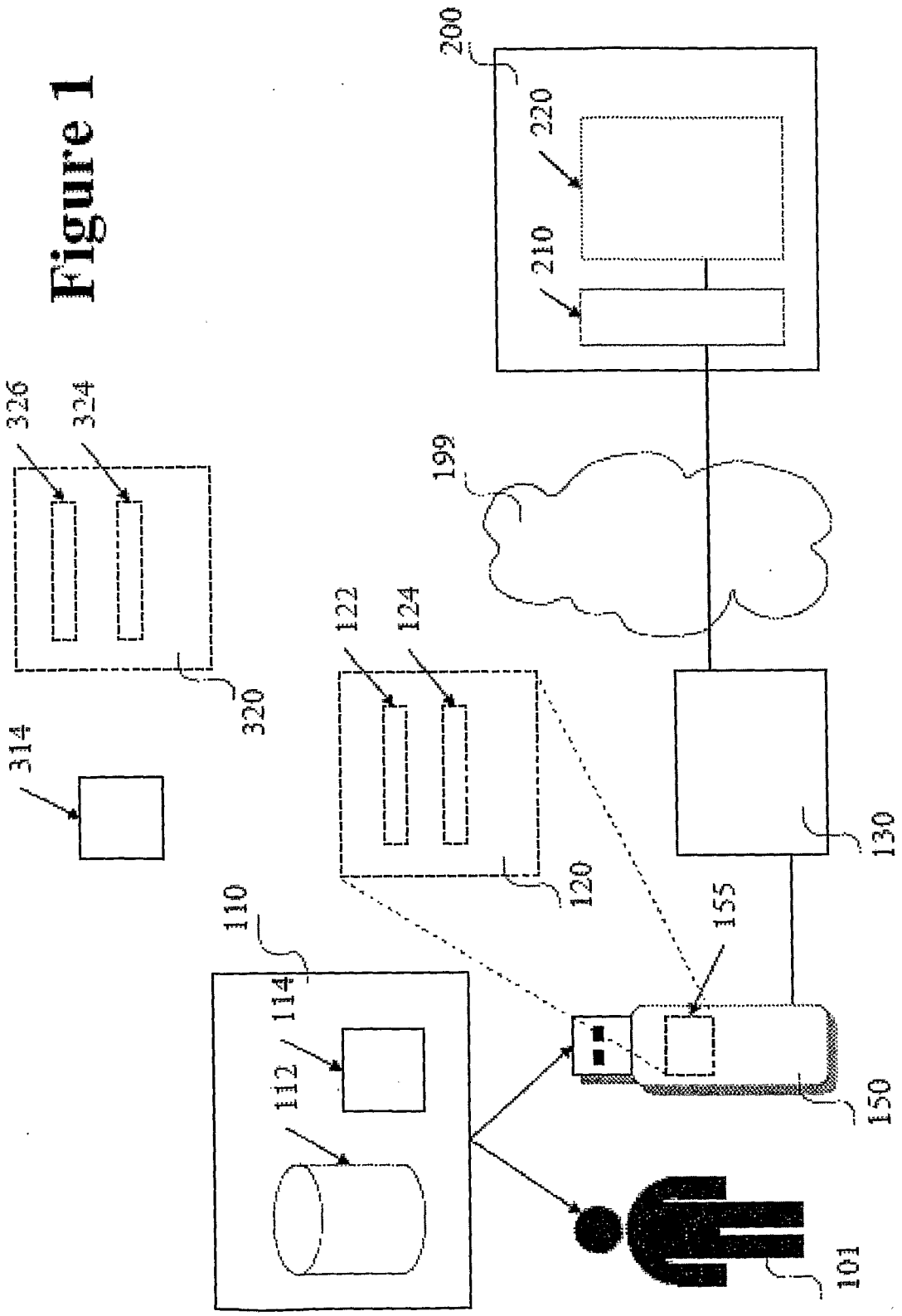
16. The storage device of any one of claims 13 to 15, wherein the storage device has a cryptographic function for generating Public Key / Private Key pairs, such that following generation the Private Key never leaves the confines of the storage device.

17. A computer program element comprising computer program code means to make a computer execute a procedure for controlling access to an electronically accessible resource, the computer program element comprising:

computer program code means for obtaining from a user a Public Key Certificate; and

computer program code means for verifying whether the user is eligible to access the electronically accessible resource by determining whether said signed Public Key Certificate includes data indicating that the user is a member of the defined demographic group, and determining whether the Public Key Certificate has been signed by or on behalf of a Trusted Third Party trusted to attest to the user being a member of the defined demographic group.

Figure 1


200
220
210
199
326
324
320
314
122
124
120
130
110
114
112
155
150
101

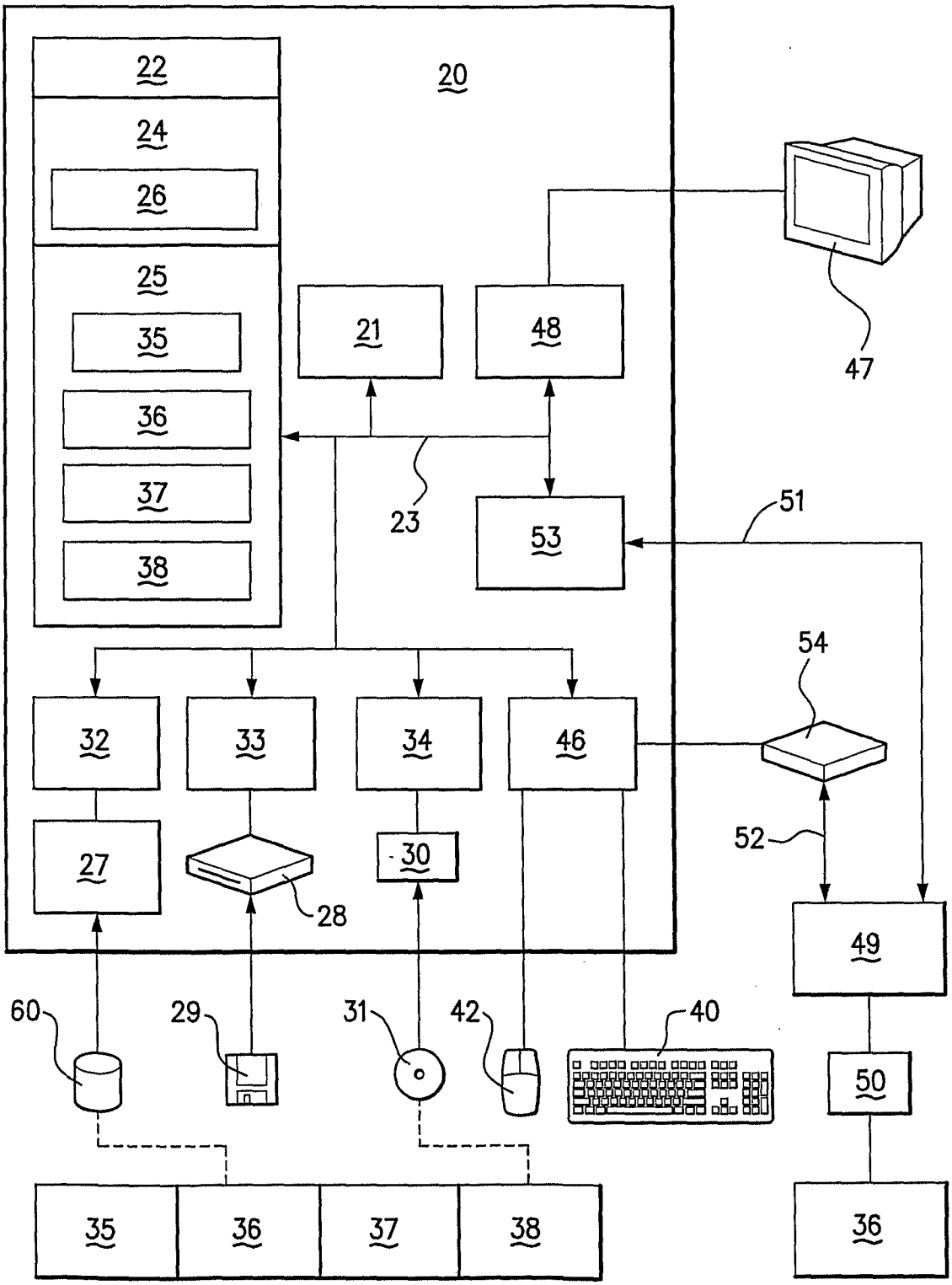

22
20
24
26
25
35
36
37
38
21
48
47
23
53
51
54
32
33
34
46
27
28
30
52
49
60
29
31
42
40
50
35
36
37
38
36

**Figure 2**

**INTERNATIONAL SEARCH REPORT**

International application No.
**PCT**/AU2008/001392

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

***H04L 9/32*** (2006.01) ***G06F 12/00*** (2006.01)

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)

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 practicable, search terms used)
EPODOC, DWPI, GOOGLE: DEMOGRAPHIC, ACCESS, CONTROL, VERIFICATION, PROVIDER, ROOT, AGE, CERTIFICATE, AUTHORITY, ANONYMOUS; and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X<br>Y | JP2001188757 A (NIPPON TELEGRAPH & TELEPHONE) 10 July 2001<br>(Machine translation, retrieved 25 November 2008 from internet) <URL: http://www4.ipdl.inpit.go.jp/Tokujitu/PAJdetail.ipdl?N0000=60&N0120=01&N2001=2&N3001=2001-188757<br>Abstract, Fig 4, paragraph [0005]-[0013],[0030]-[0033] | 1-13, 17<br>14-16 |
| P,A | US2008/0168548 A1 (O'BRIEN) 10 July 2008<br>Abstract, Fig 1-3, paragraph [0029]-[0039] | 1, 2, 6, 11-17 |
| A | US6704787 B1 (UMBREIT) 9 March 2004<br>Abstract | 1-17 |
| Y | AU2004201058 B1 (LOCKSTEP CONSULTING) 9 September 2004<br>Abstract, Figure 1 (item 10) | 14-16 |

[X] Further documents are listed in the continuation of Box C [X] 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 application or patent 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 |
|---|---|
| 24 November 2008 | 1 - DEC 2008 |
| Name and mailing address of the ISA/AU<br>AUSTRALIAN PATENT OFFICE<br>PO BOX 200, WODEN ACT 2606, AUSTRALIA<br>E-mail address: pct@ipaustralia.gov.au<br>Facsimile No. +61 2 6283 7999 | Authorized officer<br>**I.G. BIGGS**<br>AUSTRALIAN PATENT OFFICE<br>(ISO 9001 Quality Certified Service)<br>Telephone No : +61 2 6225 6118 |

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2008/001392

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US2006/0047725 A1 (BRAMSON) 2 March 2006<br>Abstract | 1-17 |

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.
**PCT/AU2008/001392**

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

| Patent Document Cited in Search Report | | Patent Family Member | | | | | |
|---|---|---|---|---|---|---|---|
| JP | 2001188757 | NONE | | | | | |
| US | 2008/168548 | NONE | | | | | |
| US | 6704787 | US | 7275110 | US | 2003/131102 | | |
| AU | 2004201058 | AU | 2005220988 | EP | 1730880 | US | 2007/245144 |
| | | WO | 2005/088899 | | | | |
| US | 2006/047725 | CA | 2578379 | WO | 2006/021088 | | |

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX