

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
20 October 2005 (20.10.2005)

PCT

(10) International Publication Number
WO 2005/098630 A1

(51) International Patent Classification⁷: **G06F 12/14**

(21) International Application Number:
PCT/AU2005/000522

(22) International Filing Date: 11 April 2005 (11.04.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2004100268 9 April 2004 (09.04.2004) AU

(71) Applicant (for all designated States except US): **LOCK-STEP CONSULTING PTY LTD** [AU/AU]; 11 Minnesota Avenue, Five Dock, NSW 2046 (AU).

(72) Inventor; and

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

(74) Agent: **F B RICE & CO**; 139 Rathdowne Street, Carlton, Victoria 3053 (AU).

(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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, 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.

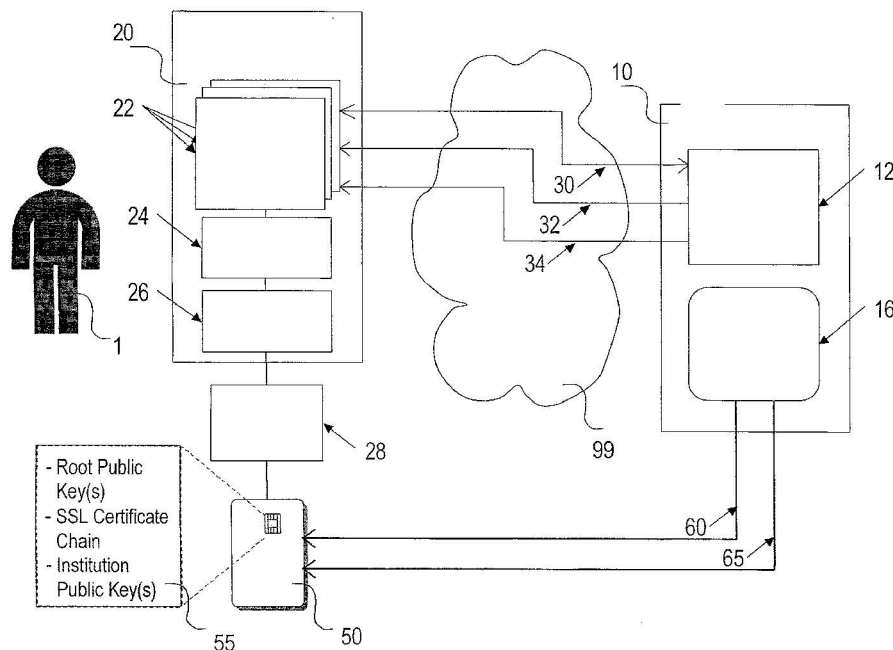
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, 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).

Published:

— with international search report

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

(54) Title: MEANS AND METHOD OF USING CRYPTOGRAPHIC DEVICES TO COMBAT ONLINE INSTITUTION IDENTITY THEFT



(57) Abstract: Customers of institutions which engage in e-business are issued with tamper resistant smart cards which include among other things a cryptographic public key of the institution. When the customer communicates with the institution on-line the customer uses the smart card to challenge the identity of the on-line business interface. Ghost web sites, bogus e-mails and unauthorised, modified or corrupted data are thereby identified effectively combating any attempted theft of the institution's on-line identity.

WO 2005/098630 A1

"Means and method of using cryptographic devices to combat online institution identity theft"

Technical Field

The present invention relates to the conduct of electronic business, and in particular to reducing the incidence of perpetration of identity theft against an institution when electronically conducting business with a customer.

Background Art

Institutions which conduct electronic business can suffer from a number of types of identity fraud where an attacker assumes the identity of the institution. Such identity fraud includes:

- establishing a bogus "ghost" web site that mimics the institution's genuine web site, and thereby defrauds customers using the ghost site instead of the genuine site;
- sending a bogus e-mail to a customer, purporting to be from the institution, to elicit personal information such as account details, which may subsequently be misused; and
- corrupting critical data such as official notices or computer program code distributed by an institution to its customers.

A range of cryptographic security technologies are in use for helping customers of an institution verify the identity of that institution when transacting with it electronically. Yet certain of these counter-measures, including "Secure Sockets Layer" (SSL) and "Object Signing", described further in the following, are now being subverted by attackers who would seek to perpetrate identity fraud against electronic business institutions.

Electronic business web sites are particularly vulnerable to attack by "ghosting". In general, ghosting is effected by an attacker corrupting the mapping of web site domain names onto physical computer addresses, so that when a customer visiting the ghosted web site believes they are connected to a certain web server associated with the domain name, he or she is in fact connected to an illegitimate server controlled by the attacker. If programmed so as to resemble the legitimate web site, the attacker's server can be used to defraud the unsuspecting customer.

One particularly widespread security technology is the "Secure Sockets Layer" (SSL) protocol, which is used in part to combat ghosting. SSL involves issuing the legitimate owner of a domain name with a digital certificate, and installing the certificate on a web server controlled by that owner. The so-called server certificate

includes the precise domain name for the web server, and is digitally signed by the certificate issuer. The digital signature on the server certificate makes the server certificate itself effectively tamper resistant. The identity and legitimacy of a certificate issuer is typically conveyed by another digital certificate issued by a higher level issuer.

5 Thus a chain of digital certificates extends from the server certificate back through a series of certificate issuers. Each digital certificate in the chain is digitally signed by its respective issuer. The certificate chain terminates with a "Root Public Key" certificate. If a given Root Public Key can be trusted as legitimate then all server certificates from issuers that are found to chain back to the trusted Root Public Key can also be trusted.

10 Many web browser applications have a so-called "Trust List" of trusted Root Public Keys, stored in computer memory, and used by browser software during the process of establishing each new SSL-secured web session. The Trust List is usually held on magnetic disc and/or random access memory. A Trust List may be pre-loaded into the web browser software by the browser manufacturer. The Trust List is usually
15 also modifiable by the user, so that new Root Public Keys may be added at the user's discretion in order to support other certificate issuers.

During the process of establishing a connection to an SSL-secured web site, a web browser using the SSL protocol will perform a series of steps which help in part to determine the legitimacy of the web site. First, the web browser will check if a server
20 certificate is installed on the web server. The web browser then scans the server certificate's contents and checks if the domain name listed in the certificate matches the expected domain name of the web site being visited. Finally, the web browser verifies that the server certificate chains back to a trusted Root Public Key certificate. If all these checks pass, then the browser establishes a secure web session with the web
25 server. Browser software typically indicates to its user that the current web session is secure by displaying a padlock graphic or similar icon.

Wherever Root Public Keys, such as those that underpin SSL, are held in magnetic disc and/or random access memory, the Root Public Keys are vulnerable to a range of potential attacks from those who may seek to defraud electronic business
30 users. One class of such vulnerabilities relates to ways in which Public Keys may be surreptitiously substituted by an attacker, thus subverting the protections offered by SSL.

One form of surreptitious Public Key substitution entails the attacker manipulating the Root Public Key Trust List. The formats of common browsers' Trust
35 Lists are readily discernible by technically skilled attackers from generally available software specifications and/or by "reverse engineering" the browser software. Armed

with knowledge of the format of a Trust List, an attacker can substitute bogus Root Public Key values. Said substitution can be effected by a variety of means, including computer viruses. The effect of inserting a bogus Root Public Key value into a browser Trust List is that SSL sessions can be established with ghosted web sites featuring
5 counterfeit server certificates that chain back to the bogus Root Public Key, thus making the ghosted sites appear legitimate to the web browser and to unsuspecting users.

Another form of surreptitious Public Key substitution is known in the field of computer security as a "Man In The Middle" attack. This form of attack does not
10 require substitution of Root Public Key values into a browser Trust List. Instead, it takes advantage of a known vulnerability in some browser software wherein the software places no restrictions on the length of the certificate chain from the server certificate back to a Root Public Key. Under these conditions, an attacker can obtain a certificate from a legitimate certificate issuer, use that certificate – termed the "Man In
15 The Middle" certificate – to illicitly spawn a bogus certificate issuer, and use the bogus certificate issuer to create illegitimate server certificates. Most web browsers, when directed to a ghosted web site featuring such an illegitimate server certificate, will establish an SSL session merely because the Man In The Middle certificate is found to chain back to a trusted Root Public Key, albeit via an additional certificate. Thus the
20 user may be led to believe that the ghosted web site is genuine.

One solution to this type of Man In The Middle attack is to tighten the rules used in browser software to check the certificate chain. For instance, browser software could be configured to only allow a certain number of certificates in the chain from the server certificate back to a Root Public Key in the Trust List. An attempted Man In
25 The Middle attack under these conditions would be detected because the attack increases the certificate chain length by one. However, this type of defence against SSL Man In The Middle attacks is complicated by the fact that different certificate issuers prefer to use intrinsically different certificate chain lengths, for example to provide operational flexibility. This means that different web server certificates will
30 exhibit different chain lengths, depending on the operational details of the respective server certificate issuers. It is therefore difficult to define a maximum certificate chain length which is characteristic of all legitimate web sites. A more robust defence against SSL Man In The Middle attacks is to ensure that the certificate chain for a given web site cannot be interfered with, no matter how long that chain might be.

35 Vulnerabilities relating to Public Key substitution affect not only SSL. Other cryptographic technologies are also vulnerable, including Object Signing (also known

as Code Signing). Object Signing is a technique for protecting a given data object (such as a piece of executable program code) against unauthorised modification. The data object to be protected has a digital signature created for it at the time it is published. Subsequently, whenever a copy of that data object is to be installed in a computer, the operating system verifies the digital signature against the contents of the data object in order to detect if the contents have changed since the time it was published. In similar fashion to SSL, the digital certificate used by any publisher to sign their data object(s) must chain back to a trusted Root Public Key. Therefore, Object Signing is vulnerable to the same types of attack as SSL, with the effect that an attacker can surreptitiously introduce illegitimate software including viruses and so-called "spy-ware" into an end user's computer, without triggering Object Signing safeguards.

A further type of identity fraud is known as "phishing", whereby e-mail purporting to be from an institution is sent by an attacker to customers of that institution. Such email may appear genuine, and can seek to elicit personal details such as account numbers and passwords, or can direct customers to web sites that may be ghost sites or may otherwise harm the customer's computer. Counter-measures against phishing may incorporate cryptographic technologies that encrypt legitimate communications from institutions to their customers, and/or authenticate the sender of said communications. However, once again, common Internet and e-commerce applications today do not offer sufficiently robust protection against Public Key substitution in order to support cryptographic defences against phishing.

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 a first party to verify an identity of a second party in an electronic communication environment, the method comprising:

5 storing in a tamper resistant storage device held by the first party at least one cryptographic Public Key associated with at least one electronic security protocol of the second party; and

verifying to the first party the identity of the second party by using the at least one cryptographic Public Key stored on the tamper resistant storage device in
10 accordance with the at least one electronic security protocol.

According to a second aspect the present invention provides a system for a first party to verify an identity of a second party in an electronic communication environment, the system comprising:

a tamper resistant storage device held by the first party and storing at least one
15 cryptographic Public Key associated with at least one electronic security protocol of the second party; and

means for verifying to the first party the identity of the second party by using the at least one cryptographic Public Key stored on the tamper resistant storage device in accordance with the at least one electronic security protocol.

20 According to a third aspect the present invention provides a client software application for verifying an identity of a second party in an electronic communication environment, the client software application comprising:

code for verifying the identity of the second party by using at least one cryptographic Public Key stored on a tamper resistant storage device in accordance
25 with at least one electronic security protocol of the second party.

According to a fourth aspect the present invention provides a tamper resistant storage device storing at least one cryptographic Public Key associated with at least one electronic security protocol of a second party, the tamper resistant storage device for use by a first party in verifying the identity of the second party by using the at least one
30 cryptographic Public Key stored on the tamper resistant storage device in accordance with the at least one electronic security protocol.

Storage of the cryptographic Public Key in a tamper resistant device, such as a smart card, obviates the need to rely on a Public Key stored in a Trust List on magnetic disc or random access memory. Hence, even should an attacker alter entries in any
35 such Trust List, a trusted Public Key can be obtained from the tamper resistant storage device. Thus, in accordance with the present invention, a tamper resistant storage

device in the possession of the first party provides a trusted copy of the cryptographic Public Key of the second party. Accordingly, the invention makes use of removable and/or portable tamper resistant cryptographic devices such as smartcards to protect an institution's cryptographic Public Key(s), and in turn to improve the cryptographic security of Internet and e-commerce applications.

Accordingly, embodiments of the present invention may substantially alleviate the broad problem of Public Key substitution, by safeguarding certain Public Keys of the institution within the tamper resistant storage device. That is, embodiments of the present invention may enable alleviation of security concerns surrounding several classes of online institution identity fraud, including ghosting, Man in the Middle attacks, and phishing.

The present invention is further particularly advantageous where the second party, such as a health institution, has in any event already issued a tamper resistant storage device to the first party. That is, the present invention recognises that tamper resistant cryptographic devices such as smartcards are becoming increasingly widespread for various reasons, particularly protection against personal identity theft perpetrated against institutions' customers. Unlike magnetic stripe cards, smartcards and functionally similar removable cryptographic devices are very difficult to duplicate, and are thus considered to be tamper resistant storage devices in accordance with the present invention. For example, information held within the internal memory of a "smart" cryptographic device generally cannot be accessed without first presenting a correct personal identification number (PIN). In some cryptographic devices certain data, such as cryptographic Private Keys, are prevented by the device's internal operating system from ever being transmitted from the device. Such a cryptographic device cannot be duplicated by an attacker even if the attacker has gained knowledge of the device's PIN. These properties of such portable cryptographic devices (and in particular smartcards) in effect make them immune to "skimming", being the form of identity theft where magnetic stripe cards are illicitly duplicated by copying data directly from one card's stripe to another's.

The present invention has recognised that smartcards and other functionally similar tamper resistant portable cryptographic devices are also becoming increasingly desirable, and increasingly issued by institutions to their customers, due to steadily enhanced levels of support in standard Internet software, operating systems and commercial computer hardware. For example, credit card companies have announced that in future, magnetic stripe card technology must be replaced by smartcard technology. Therefore, the present invention takes advantage of the recognition that

customers of online institutions, especially financial institutions, will in future carry smartcards or other functionally similar removable cryptographic devices with which to authenticate themselves for access to electronic business services.

That is, the present invention recognises that, not only may such smartcards be
5 used to prevent customer identity theft in the manner set out in the preceding, but that the customer-carried smartcard may be used by an institution to protect their own online identity. Advantageously, such protection may be afforded to the institution by use of existing customer smartcards for storage of the institution's Public Key, in accordance with the present invention, whether or not that smartcard was issued by the
10 institution. Accordingly, in instances where the first party such as a customer already holds a suitable tamper resistant storage device in which the Public Key of the second party such as an institution may be stored, no additional infrastructure in the way of additional smartcards is required. Rather, the second party or institution needs merely to arrange for a trusted copy of the Public Key to be stored within the existing tamper
15 resistant storage device of the first party or customer.

The tamper resistant storage device may further store other cryptographic elements, such as SSL digital certificate chains, Root Public Keys and/or multiple institution Public Keys.

Furthermore, in some embodiments of the invention a smartcard or other tamper
20 resistant storage device issued by or on behalf of a first institution may be used to store one or more trusted Public Keys of other parties or institutions. Thus, in some such embodiments the tamper resistant storage device may hold a plurality of trusted Public Keys relating to a plurality of institutions.

In embodiments of the invention the first party may be a client and the second
25 party may be a server. For example the client may be client software operating on a computing platform, operating in conjunction with a tamper resistant storage device.

In further embodiments of the invention the first party may be a customer and the second party may be a business. For example the second party may be any one or more of a credit card provider, a health institution, a government agency, a
30 telecommunications company, a licensing body, a gaming body, a software publisher, a software distributor, a merchant, and a financial institution.

In embodiments of the invention, the tamper resistant storage device may comprise a portable device having an in built security module, for example a smartcard, a subscriber identity module (SIM card), a cryptographic universal serial bus (USB)
35 storage device; and/or a wireless portable computing device with tamper resistant storage, such as a Blackberry®.

In preferred embodiments the tamper resistant storage device is a portable and removable device to be held by a customer. In such embodiments, the tamper resistant storage device preferably communicates with application software through logical, communications and physical interfaces to enable use of the Public Key by the application software in accordance with the electronic security protocol. The physical interface may be a contact smartcard reader, a contactless smartcard reader, a wireless network interface, USB port, serial port, parallel port, or SIM card receptacle. The communications interface may include software drivers for a device reader. The logical interface may be an application programming interface to provide application software with the means to make use of cryptographic keys and other data held securely within the tamper resistant storage device.

In embodiments of the invention, application software of the first party may make use of the Public Key of the second party by making a temporary copy of the Public Key outside the tamper resistant storage device. Alternatively, the application software may feed data into the tamper resistant storage device causing functions to be executed within the device so that the Public Key need not leave the device.

It will be appreciated that the present invention provides for secure storage of a Public Key for use in any applicable electronic security protocol. For example the electronic security protocol may be one or more of Secure Multipurpose Internet Mail Extensions (S/MIME), Pretty Good Privacy (PGP), Open Standard for Pretty Good Privacy (OpenPGP), Privacy Enhancements for Internet Electronic Mail (PEM), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Wireless Transport Layer Security (WTLS), Extensible Markup Language (XML) Signatures, Internet Protocol Security (IPSEC), Authenticode™ object signing, Java Archive (JAR) object signing, Visual Basic for Applications (VBA) object signing, and Netscape Navigator object signing.

According to a fifth aspect the present invention provides a means of protecting an electronic business institution from identity theft, said means comprising removable cryptographic devices issued to the institution's customers, and application programming interfaces, where said removable devices contain tamper-resistant copies of cryptographic Public Keys of the institution, said Public Keys being associated with standard electronic business security functions used by the institution to transact with its customers.

In some embodiments of the invention copies of one or more certificates in the digital certificate chain for an SSL-secured web site, from the Root Public Key through

to the server certificate, may be stored in the removable cryptographic device and verified by application software when establishing an SSL session.

In further embodiments of the invention a copy of a Public Key of the institution may be stored in the removable cryptographic device and used to verify secure e-mail
5 sent by the institution.

In still further embodiments of the invention a copy of a Public Key of the institution may be stored in the removable cryptographic device and used to verify digitally signed data objects sent by the institution.

According to a sixth aspect, the present invention provides a method of
10 protecting an electronic business institution from identity theft, said method comprising the steps of making available to customers copies of cryptographic Public Keys of the institution, storing said Public Keys in tamper-resistant removable cryptographic devices, and having customers' application software utilise the Public Keys in said removable cryptographic devices to effect standard electronic business security
15 functions.

Brief Description of the Drawing

By way of example only, a preferred embodiment of the invention will be described with reference to the accompanying drawing which illustrates
20 implementation of the present invention in providing secure electronic communications between a customer and an institution.

Detailed Description of the Invention

With reference to Figure 1, an online Institution 10 and a Customer 1 of said
25 institution transact with one another over a Communications Network 99 using a Web Server 12 and one or more Internet Applications 22 running on the Customer's Computer 20. The Internet Applications 22 can (without limitation) include web browser, e-mail, and/or special purpose transaction software written by or on behalf of the Institution 10. In a preferred embodiment, Internet Applications 22 interface to a
30 Smartcard 50 via a Smartcard Reader 28, Smartcard Reader Driver software 26 and a Cryptographic Application Programming Interface (Crypto API) 24. The Crypto API 24 software enables Internet Applications 22 to make use of cryptographic keys stored within the Smartcard 50 instead of keys customarily stored elsewhere in memory in the Customer Computer 20, where said keys would be vulnerable to substitution
35 attacks.

Still referring to Figure 1, three types of low level electronic security function are illustrated, any or all of which are utilised by the Internet Applications 22 in order to effect high level transactions between the Institution 10 and its Customer 1, the three types of low level security function being:

- 5 i. Secure Sockets Layer (SSL) 30 which allows secure web sessions to be conducted by the Customer 20 on the Institution's Web Server 12.
- ii. Secure E-mail 32 which allows the Institution 10 and Customer 1 to exchange encrypted and/or authenticated electronic messages quickly and economically; in particular, in respect of a preferred embodiment,
- 10 the Institution 10 uses Secure E-mail 32 to send important notices to its Customer 1 in order to combat phishing.
- iii. Signed Objects 34 which allow the Institution 10 to send particular data objects to the Customer 1 (including without limitation software upgrades, text of important notices and business data files) where
- 15 standard Object Signing verification functions in the operating system of the Customer Computer 20 can check the veracity and integrity of said data objects before the objects are installed.

In a preferred embodiment, the Institution 10 issues and distributes 60 a Smartcard 50 to the Customer 1. The Smartcard 50 is pre-loaded by (or on behalf of)

20 the Institution 10 with one or more Public Keys 55, all held in the Smartcard's tamper resistant memory. Said Public Keys are organised in standard Public Key Certificate formats. The Public Keys so held may include any or all of the following:

- A copy of the Root Public Key of each trusted certificate issuer used by the Institution 10; in the preferred embodiment Root Public Keys
- 25 stored in the Smartcard 50 are used by Internet Applications 22 instead of any customary Trust List stored elsewhere in memory in the Customer Computer 20.
- A copy of the entire digital certificate chain from Root Public Key through to server certificate for the SSL-secured Web Server 12.
- 30 - A copy of a Public Key to be used to decrypt Secure E-mails 32 sent by the Institution 10 to Customer 1 in order to verify that said Secure E-mail did indeed originate from the Institution 10.
- A copy of a Public Key to be used to verify the digital signature on Secure E-mails 32 sent by the Institution 10 to Customer 1.
- 35 - A copy of a Public Key to be used to verify the digital signature of Signed Objects 34 sent by the Institution 10 to Customer 1.

The invention improves the security of the low level electronic business security functions SSL, Secure E-mail and Object Signing as used by the Institution 10, by storing in the Smartcard 50 all Public Keys used by said low level functions. When thus stored in a tamper-resistant Smartcard 50, said Public Keys cannot be readily
5 substituted or otherwise interfered with by an attacker. Whenever Internet Applications 22 need to verify the origin of a Secure E-mail 32 or a Signed Object 34, the application software uses the necessary Public Keys 55 in the Smartcard 50.

Further, to protect against Man In The Middle attacks on SSL, whether before, during or after establishment of a standard SSL session 30, Internet Applications 22 can
10 verify that the certificate chain for the Web Server 12 matches the SSL certificate chain 55 stored in the Smartcard 50. If the certificate chains are found not to match, then the web site can be assumed to be a ghost site, and the application software can terminate the web session before any harm can be done by the ghost web server.

Further, to protect against phishing, the Institution 10 can use Secure E-mail 32
15 to effect important business communications with Customer 1 and/or Object Signing 34 to protect important business information against attack.

From time to time, for operational reasons or because digital certificates expire, the Institution 10 will need to replace or renew its various Public Keys. At such times, the Institution 10 can inject copies of all new Public Key data 55 into the Smartcard 50
20 via a standard secure protocol for Smartcard Data Download 65. Several standard methods are available for such secure data download, as will be appreciated by persons skilled in computer security. The efficacy of the present invention does not depend on the details of whatever secure data download method is used in the renewal of the institution's Public Keys.

More generally, 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. It will be particularly appreciated that the present invention can be constructed using a variety of alternate but standard components for
30 the application software, smartcard or functionally similar removable cryptographic device, removable cryptographic device reader, and/or reader drivers, without materially affecting the efficacy of the invention in respect of combating online institution identity fraud through protection of Public Keys of the institution used in low level security functions. Further, it will be realised that a variety of removable
35 cryptographic devices are available with similar functions in respect of secure storage of cryptographic keys but packaged in different forms, including without limitation

plastic cards with embedded integrated circuit chip and Universal Serial Bus (USB) tokens or “smart keys”, and that the present invention can be constructed from such alternate devices without affecting the scope or spirit of the invention in regard to protecting an institution’s Public Keys and securely making them available to the
5 institution’s customers. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS:

1. A method for a first party to verify an identity of a second party in an electronic communication environment, the method comprising:
 - storing in a tamper resistant storage device held by the first party at least one
 - 5 cryptographic Public Key associated with at least one electronic security protocol of the second party; and
 - verifying to the first party the identity of the second party by using the at least one cryptographic Public Key stored on the tamper resistant storage device in accordance with the at least one electronic security protocol.
- 10 2. The method of claim 1 wherein information stored in the tamper resistant storage device can be accessed only by presenting a correct personal identification number (PIN).
3. The method of claim 1 or claim 2 wherein certain data is prevented by an internal operating system of the tamper resistant storage device from ever being
- 15 transmitted from the device.
4. The method of any one of claims 1 to 3 wherein the tamper resistant storage device further enables authentication of the identity of the first party.
5. The method of claim 4 wherein the tamper resistant storage device enables authentication of the identity of the first party for the electronic security protocol.
- 20 6. The method of claim 4 or claim 5 wherein the tamper resistant storage device stores a Private Key associated with the first party.
7. The method of any one of claims 1 to 6 wherein the tamper resistant storage device had been held by the first party prior to the storing of the cryptographic Public Key.
- 25 8. The method of claim 7 wherein the tamper resistant storage device had been previously issued to the first party by the second party to enable authentication of the identity of the first party to the second party.
9. The method of claim 7 wherein the tamper resistant storage device had previously been issued to the first party by a third party.
- 30 10. The method of any one of claims 1 to 6 wherein the tamper resistant storage device is issued to the first party after the storing of the cryptographic Public Key.
11. The method of any one of claims 1 to 10 wherein the tamper resistant storage device stores a plurality of trusted Public Keys relating to a plurality of institutions.
12. The method of any one of claims 1 to 11 wherein the first party comprises a
- 35 client and the second party comprises a server.

13. The method of claim 12 wherein the client comprises client software operating on a computing platform in conjunction with the tamper resistant storage device.

14. The method of any one of claims 1 to 13 wherein the first party comprises a customer and the second party comprises a business.

5 15. The method of claim 14 wherein the second party comprises at least one of a credit card provider, a health institution, a government agency, a telecommunications company, a licensing body, a gaming body, a software publisher, a software distributor, a merchant, and a financial institution.

10 16. The method of any one of claims 1 to 15 wherein the tamper resistant storage device comprises at least one of a smartcard, a subscriber identity module (SIM card), a cryptographic universal serial bus (USB) storage device and a wireless portable computing device with tamper resistant storage.

17. The method of any one of claims 1 to 16, wherein the electronic security protocol comprises at least one of Secure Multipurpose Internet Mail Extensions (S/MIME), Pretty Good Privacy (PGP), Open Standard for Pretty Good Privacy (OpenPGP), Privacy Enhancements for Internet Electronic Mail (PEM), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Wireless Transport Layer Security (WTLS), Extensible Markup Language (XML) Signatures, Internet Protocol Security (IPSEC), Authenticode™ object signing, Java Archive (JAR) object signing, Visual
15 Basic for Applications (VBA) object signing, and Netscape Navigator object signing.

18. The method of any one of claims 1 to 17, further comprising storing in the tamper resistant storage device at least one of a Root Public Key and a security protocol certificate chain.

19. The method of any one of claims 1 to 18 wherein using the at least one
25 cryptographic Public Key to verify the identity of the second party comprises communicating the cryptographic Public Key from the tamper resistant storage device via a device interface to a software application.

20. The method of any one of claims 1 to 18 wherein using the at least one cryptographic Public Key to verify the identity of the second party comprises causing
30 functions to be executed within the tamper resistant storage device without the cryptographic Public Key leaving the tamper resistant storage device.

21. A system for a first party to verify an identity of a second party in an electronic communication environment, the system comprising:

a tamper resistant storage device held by the first party and storing at least one
35 cryptographic Public Key associated with at least one electronic security protocol of the second party; and

means for verifying to the first party the identity of the second party by using the at least one cryptographic Public Key stored on the tamper resistant storage device in accordance with the at least one electronic security protocol.

22. The system of claim 21 wherein information stored in the tamper resistant storage device can be accessed only by presenting a correct personal identification number (PIN).

23. The system of claim 21 or claim 22 wherein certain data is prevented by an internal operating system of the tamper resistant storage device from ever being transmitted from the device.

24. The system of any one of claims 21 to 23 wherein the tamper resistant storage device further enables authentication of the identity of the first party.

25. The system of claim 24 wherein the tamper resistant storage device enables authentication of the identity of the first party for the electronic security protocol.

26. The system of claim 24 or claim 25 wherein the tamper resistant storage device stores a Private Key associated with the first party.

27. The system of any one of claims 21 to 26 wherein the tamper resistant storage device had been held by the first party prior to the storing of the cryptographic Public Key.

28. The system of claim 27 wherein the tamper resistant storage device had been previously issued to the first party by the second party to enable authentication of the identity of the first party to the second party.

29. The system of claim 27 wherein the tamper resistant storage device had previously been issued to the first party by a third party.

30. The system of any one of claims 21 to 26 wherein the tamper resistant storage device is issued to the first party after the storing of the cryptographic Public Key.

31. The system of any one of claims 21 to 30 wherein the tamper resistant storage device stores a plurality of trusted Public Keys relating to a plurality of institutions.

32. The system of any one of claims 21 to 31 wherein the first party comprises a client and the second party comprises a server.

33. The system of claim 32 wherein the client comprises client software operating on a computing platform in conjunction with the tamper resistant storage device.

34. The system of any one of claims 21 to 33 wherein the first party comprises a customer and the second party comprises a business.

35. The system of claim 34 wherein the second party comprises at least one of a credit card provider, a health institution, a government agency, a telecommunications

company, a licensing body, a gaming body, a software publisher, a software distributor, a merchant, and a financial institution.

36. The system of any one of claims 21 to 35 wherein the tamper resistant storage device comprises at least one of a smartcard, a subscriber identity module (SIM card), a
5 cryptographic universal serial bus (USB) storage device and a wireless portable computing device with tamper resistant storage.

37. The system of any one of claims 21 to 36, wherein the electronic security protocol comprises at least one of Secure Multipurpose Internet Mail Extensions (S/MIME), Pretty Good Privacy (PGP), Open Standard for Pretty Good Privacy
10 (OpenPGP), Privacy Enhancements for Internet Electronic Mail (PEM), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Wireless Transport Layer Security (WTLS), Extensible Markup Language (XML) Signatures, Internet Protocol Security (IPSEC), Authenticode™ object signing, Java Archive (JAR) object signing, Visual Basic for Applications (VBA) object signing, and Netscape Navigator object signing.

15 38. The system of any one of claims 21 to 37, further comprising storing in the tamper resistant storage device at least one of a Root Public Key and a security protocol certificate chain.

39. The system of any one of claims 21 to 38 wherein the at least one cryptographic Public Key is used to verify the identity of the second party by communication of the
20 cryptographic Public Key from the tamper resistant storage device via a device interface to a software application.

40. The system of any one of claims 21 to 38 wherein the at least one cryptographic Public Key is used to verify the identity of the second party by executing functions within the tamper resistant storage device without the cryptographic Public Key leaving
25 the tamper resistant storage device.

41. A client software application for verifying an identity of a second party in an electronic communication environment, the client software application comprising:
code for verifying the identity of the second party by using at least one
cryptographic Public Key stored on a tamper resistant storage device in accordance
30 with at least one electronic security protocol of the second party.

42. The client software application of claim 41 wherein information stored in the tamper resistant storage device can be accessed only by presenting a correct personal identification number (PIN).

43. The client software application of claim 41 or claim 42 further comprising code
35 for using the tamper resistant storage device to authenticate the identity of the first party.

44. The client software application of claim 43 wherein the identity of the first party is authenticated for the electronic security protocol.

45. The client software application of claim 43 or claim 44 comprising code for using a Private Key associated with the first party stored in the tamper resistant storage device.

46. The client software application of any one of claims 41 to 45 comprising code for using a plurality of trusted Public Keys relating to a plurality of institutions stored within the tamper resistant storage device.

47. The client software application of any one of claims 41 to 46 wherein the second party comprises a server.

48. The client software application of any one of claims 41 to 47 wherein the second party comprises a business.

49. The client software application of claim 48 wherein the second party comprises at least one of a credit card provider, a health institution, a government agency, a telecommunications company, a licensing body, a gaming body, a software publisher, a software distributor, a merchant, and a financial institution.

50. The client software application of any one of claims 41 to 49 wherein the tamper resistant storage device comprises at least one of a smartcard, a subscriber identity module (SIM card), a cryptographic universal serial bus (USB) storage device and a wireless portable computing device with tamper resistant storage.

51. The client software application of any one of claims 41 to 50, wherein the electronic security protocol comprises at least one of Secure Multipurpose Internet Mail Extensions (S/MIME), Pretty Good Privacy (PGP), Open Standard for Pretty Good Privacy (OpenPGP), Privacy Enhancements for Internet Electronic Mail (PEM), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Wireless Transport Layer Security (WTLS), Extensible Markup Language (XML) Signatures, Internet Protocol Security (IPSEC), Authenticode™ object signing, Java Archive (JAR) object signing, Visual Basic for Applications (VBA) object signing, and Netscape Navigator object signing.

52. The client software application of any one of claims 41 to 51, further comprising code for using at least one of a Root Public Key and a security protocol certificate chain stored in the tamper resistant storage device.

53. The client software application of any one of claims 41 to 52 wherein the at least one cryptographic Public Key is used to verify the identity of the second party by communication of the cryptographic Public Key from the tamper resistant storage device via a device interface to the client software application.

54. The client software application of any one of claims 41 to 55 comprising code for causing functions using the cryptographic Public Key to be executed within the tamper resistant storage device without the cryptographic Public Key leaving the tamper resistant storage device.
- 5 55. A tamper resistant storage device storing at least one cryptographic Public Key associated with at least one electronic security protocol of a second party, the tamper resistant storage device for use by a first party in verifying the identity of the second party by using the at least one cryptographic Public Key stored on the tamper resistant storage device in accordance with the at least one electronic security protocol.
- 10 56. The tamper resistant storage device of claim 55 wherein information stored in the tamper resistant storage device can be accessed only by presenting a correct personal identification number (PIN).
57. The tamper resistant storage device of claim 55 or claim 56 wherein certain data is prevented by an internal operating system of the tamper resistant storage device from
- 15 ever being transmitted from the device.
58. The tamper resistant storage device of any one of claims 55 to 57 wherein the tamper resistant storage device further enables authentication of the identity of the first party.
59. The tamper resistant storage device of claim 58 wherein the tamper resistant
- 20 storage device enables authentication of the identity of the first party for the electronic security protocol.
60. The tamper resistant storage device of claim 58 or claim 59 wherein the tamper resistant storage device stores a Private Key associated with the first party.
61. The tamper resistant storage device of any one of claims 55 to 60 wherein the
- 25 tamper resistant storage device had been held by the first party prior to the storing of the cryptographic Public Key.
62. The tamper resistant storage device of claim 61 wherein the tamper resistant storage device had been previously issued to the first party by the second party to enable authentication of the identity of the first party to the second party.
- 30 63. The tamper resistant storage device of claim 61 wherein the tamper resistant storage device had previously been issued to the first party by a third party.
64. The tamper resistant storage device of any one of claims 55 to 60 wherein the tamper resistant storage device is issued to the first party after the storing of the cryptographic Public Key.

65. The tamper resistant storage device of any one of claims 55 to 64 wherein the tamper resistant storage device stores a plurality of trusted Public Keys relating to a plurality of institutions.
66. The tamper resistant storage device of any one of claims 55 to 65 wherein the
5 first party comprises a client and the second party comprises a server.
67. The tamper resistant storage device of claim 66 wherein the client comprises client software operating on a computing platform in conjunction with the tamper resistant storage device.
68. The tamper resistant storage device of any one of claims 55 to 67 wherein the
10 first party comprises a customer and the second party comprises a business.
69. The tamper resistant storage device of claim 68 wherein the second party comprises at least one of a credit card provider, a health institution, a government agency, a telecommunications company, a licensing body, a gaming body, a software publisher, a software distributor, a merchant, and a financial institution.
- 15 70. The tamper resistant storage device of any one of claims 55 to 69 wherein the tamper resistant storage device comprises at least one of a smartcard, a subscriber identity module (SIM card), a cryptographic universal serial bus (USB) storage device and a wireless portable computing device with tamper resistant storage.
71. The tamper resistant storage device of any one of claims 55 to 70, wherein the
20 electronic security protocol comprises at least one of Secure Multipurpose Internet Mail Extensions (S/MIME), Pretty Good Privacy (PGP), Open Standard for Pretty Good Privacy (OpenPGP), Privacy Enhancements for Internet Electronic Mail (PEM), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Wireless Transport Layer Security (WTLS), Extensible Markup Language (XML) Signatures, Internet Protocol
25 Security (IPSEC), Authenticode™ object signing, Java Archive (JAR) object signing, Visual Basic for Applications (VBA) object signing, and Netscape Navigator object signing.
72. The tamper resistant storage device of any one of claims 55 to 71, further storing at least one of a Root Public Key and a security protocol certificate chain.
- 30 73. The tamper resistant storage device of any one of claims 55 to 72 wherein the at least one cryptographic Public Key is used to verify the identity of the second party by communication of the cryptographic Public Key from the tamper resistant storage device via a device interface to a software application.
74. The tamper resistant storage device of any one of claims 55 to 72 wherein the at
35 least one cryptographic Public Key is used to verify the identity of the second party by

executing functions within the tamper resistant storage device without the cryptographic Public Key leaving the tamper resistant storage device.

75. A means of protecting an electronic business institution from identity theft, said means comprising removable cryptographic devices issued to the institution's
5 customers, and application programming interfaces, where said removable devices contain tamper-resistant copies of cryptographic Public Keys of the institution, said Public Keys being associated with standard electronic business security functions used by the institution to transact with its customers.

76. A means according to claim 75 wherein copies of one or more certificates in the
10 digital certificate chain for an SSL-secured web site, from the Root Public Key through to the server certificate, are stored in the removable cryptographic device and verified by application software when establishing an SSL session.

77. A means according to claim 75 wherein a copy of a Public Key of the institution is stored in the removable cryptographic device and used to verify secure e-mail sent by
15 the institution.

78. A means according to claim 75 wherein a copy of a Public Key of the institution is stored in the removable cryptographic device and used to verify digitally signed data objects sent by the institution.

79. A method of protecting an electronic business institution from identity theft,
20 said method comprising the steps of making available to customers copies of cryptographic Public Keys of the institution, storing said Public Keys in tamper-resistant removable cryptographic devices, and having customers' application software utilise the Public Keys in said removable cryptographic devices to effect standard electronic business security functions.

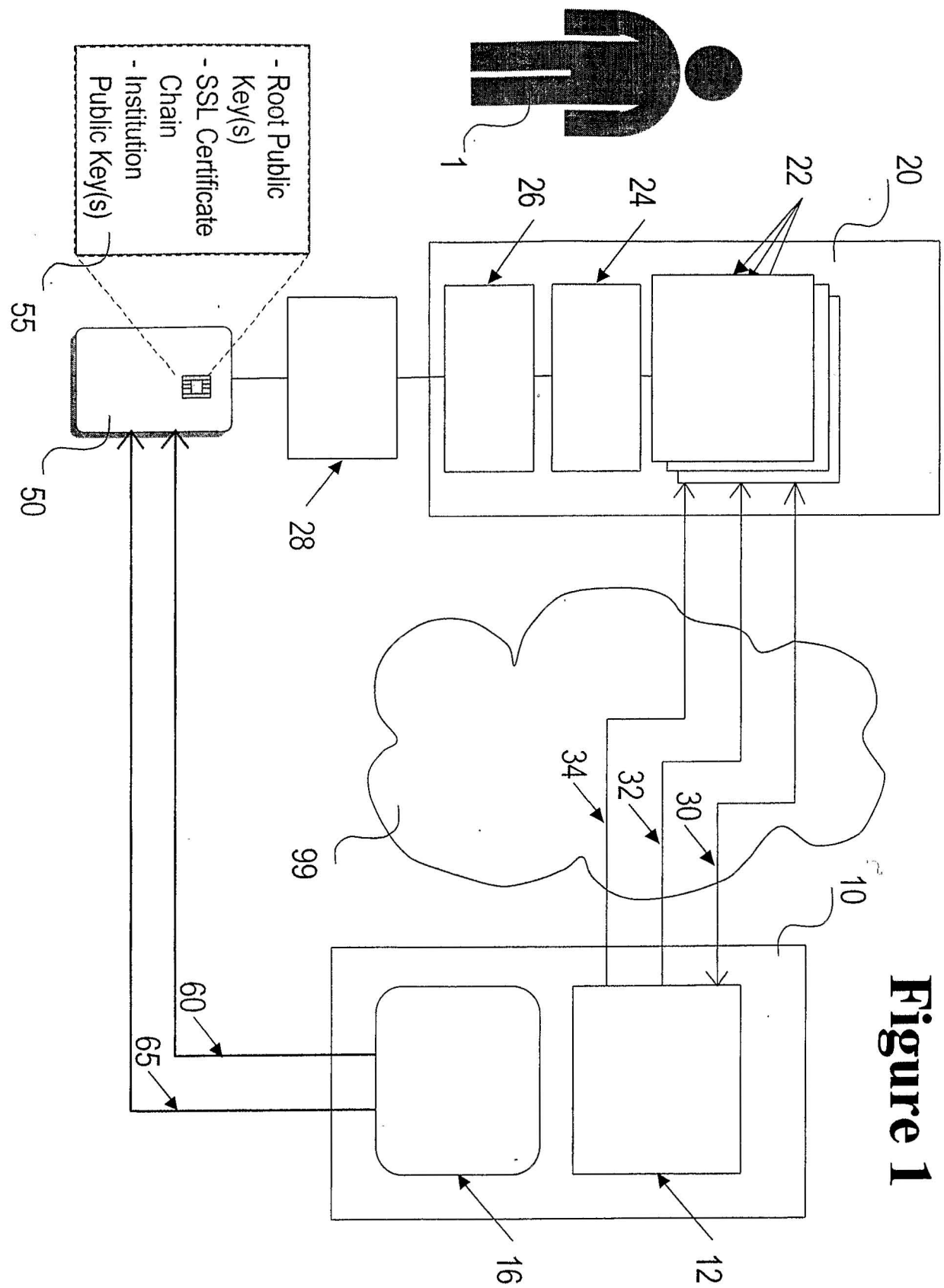
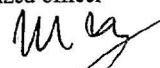


Figure 1

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU2005/000522

A. CLASSIFICATION OF SUBJECT MATTER		
Int. Cl. ⁷ : G06F 12/14		
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) USPTO, esp@cenet: spoof*, internet, "public key", "smart card", ECLA: G06F21/00, G06F21/00N5A2D		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US-6141752-A (DANCS et al.) 31 October 2000 See column 2 lines 8 to 67.	1, 4, 5, 7, 9-15, 17-19, 21, 24, 25, 27, 29-35, 37-39, 41, 43, 44, 46- 49, 51-53, 55, 58, 59, 61, 63-69, & 71-73
P, A	WO-2004/082201-A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.) 23 September 2004 See abstract	
P, A	WO-2004/075505-A1 (TELECOM ITALIA S.P.A.) 2 September 2004 See whole document	
A	US-2004/0015694-A1 (DETREVILLE) 22 January 2004 See whole document	
☒ 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 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 2 May 2005		Date of mailing of the international search report 10 MAY 2005
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustalia.gov.au Facsimile No. (02) 6285 3929		Authorized officer  MICHAEL HARDY Telephone No: (02) 6283 2547

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU2005/000522

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP-1282026-A2 (T.I.S.S. S.R.L.) 5 February 2003 See whole document	
A	US-6385729-B1 (DIGIORGIO et al.) 7 May 2002 See whole document	
A	EP-1076279-A1 (HEWLETT-PACKARD COMPANY) 14 February 2001 See whole document	
A	WO-2000/054126-A1 (HEWLETT-PACKARD COMPANY) 14 September 2000 See whole document	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/AU2005/000522

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			
US	6141752				
WO	2004082201				
WO	2004075505	AU	2003210334		
US	2004015694	US	6327652	US	6330670
		US	6820063	US	2003194094
		US	2003196099	US	2003196110
		US	2005060549	US	6609199
				US	2003196085
				US	2003196111
EP	1282026	IT	TO20010771		
US	6385729	AU	42037/99	EP	1013050
				WO	9962210
EP	1076279	EP	1203278	EP	1204910
		WO	0113199	WO	0113198
WO	0054126	EP	1030237	EP	1076280
		EP	1159662	EP	1161714
		EP	1161716	WO	0048061
		WO	0048063	WO	0054125
				EP	1159660
				EP	1161715
				WO	0048062
Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.					
END OF ANNEX					