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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 July 2002 (11.07.2002)

PCT

(10) International Publication Number
WO 02/054191 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US02/00825

(22) International Filing Date: 8 January 2002 (08.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/260,193 8 January 2001 (08.01.2001) US

(71) Applicant *(for all designated States except US)*: **STEFAAN DE SCHRIJVER, INCORPORATED** [US/US]; 952 Beacon Street, Newton, MA 02459 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **LENT, Michelle, A.** [US/US]; 1730 La Loma Avenue, Berkeley, CA 94709 (US).

(74) Agents: **LOREN, Ralph, A.** et al.; Lahive & Cockfield, LLP, 28 State Street, Boston, MA 02109 (US).

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

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

Published:
— *without international search report and to be republished upon receipt of that 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.

WO 02/054191 A2

(54) Title: PICS: APPARATUS AND METHODS FOR PERSONAL MANAGEMENT OF PRIVACY, INTEGRITY, CREDENTIALING AND SECURITY IN ELECTRONIC TRANSACTIONS

(57) Abstract: The invention concerns a PICS system that provides personal privacy and the data integrity of the credentialed consumer is kept secure, while the portal can use statistical evidence and non-private information. The occurrence of the transaction cannot be repudiated. If there is a need to verify the content of the data, both parties must participate in order to make it possible to fully decrypt the data to a clear message.

PICS: APPARATUS AND METHODS FOR PERSONAL MANAGEMENT OF PRIVACY, INTEGRITY, CREDENTIALING AND SECURITY IN ELECTRONIC TRANSACTIONS

BACKGROUND OF THE INVENTION

1. Field of The Invention

The invention relates to the field of authentication, fraud detection and prevention, security, cryptography and electronic and mobile commerce. More particularly a Privacy, Integrity, Credentialing and Security System enables users to manage themselves the privacy, credentialing, integrity, and security of their electronic records and transactions.

2. Description of The Prior Art

Today applications that allow order placement, fulfillment and payment by means of credit cards are common, whether at point of sales, or over the Internet for so-called electronic-commerce. These applications are well known in the art. They require the users to identify themselves by means of a pin code and a name, with additional information such as date of birth, mother's maiden name, (part of) a social security number, expiration date, last transaction amounts, or the like.

Service providers keep this information together with the pre-registered templates, that include address and other personal data, and with the history of the transactions. These "secrets" often are shared by the service providers, such as banks, by depositing them with third parties such as credit bureaus, an example of which is Equifax. These measures, while widely used with private networks, are not very adequate for use with open networks such as Internet, where identity easily can be stolen. Furthermore these systems are prone to errors and omissions. It is difficult for consumers, who are the subject of these secrets to know of their existence, and therefore to correct them. On top of that these secrets are often used for purposes other than credentialing. Banks and market place are known to collect and sell all or part of the information that their clients entrusted them with for mercantile purposes, with neither the knowledge nor authorization by the clients.

For the purpose of Electronic Commerce various processes have been devised for authenticating users and ensuring privacy of the data transmitted between users. Government may designate and accredit service providers to perform specific roles for secure data transmission, including digital or electronic signatures.

Electronic commerce may require several distinct security elements: authentication, secure communications, trusted third parties, electronic contracts, digital payment systems, corporate information security. Solutions to the problems include symmetric and asymmetric cryptography, public key infrastructures (PKI), and X509 certificates.

Intra company transactions and data are protected to some extent by firewalls. However most fraud occurs inside. Existing solutions for data integrity and access control are more oriented towards extranet situations than towards intra-net operations. PKI type solutions are not practical and expensive for intranet usage.

At the business-to-business (B2B) level such solutions are provided by trusted third parties, such as Identrus. This places the businesses at equal footing and Identrus, a PKI consortium of banks is in control of the transaction and the security, integrity and confidentiality issues surrounding it. Identrus provides the so-called middleware that the banks use to provide management of all security issues. The traditional banks provide a sufficient framework for legality and trust to make this solution workable as a global B2B environment.

At a consumer-to-consumer level secure socket layer and pretty good privacy are widely available, but do not provide a legal framework of trust that can be upheld in court because of the lack of uniformity in the commercial codes of various countries.

At a business-to-consumer (B2C) level the solutions are driven by the businesses, they may offer the possibilities of registering for certificates, from PKI services such as Verisign. However, the certificates issued by the PKI are not really identifying the individual who requests them, nor the individual who uses them. Also the business tends to build profiles of the users accessing the business portal. Thus Amazon.com decided to declare these profiles a corporate

asset, in order to improve its balance sheet. Trust-e is an organization that promises its members to policy privacy issues related to electronic commerce. But when Toysmart.com went into receivership, the US Commerce Department itself had to go to court to prevent Toysmart to sell its customer profiles to the highest bidder, in spite of its membership in Trust-e and its commitment to its members to maintain their privacy at all time.

It is thus not evident that either business or government will guarantee the privacy, the integrity and the security of data and transactions conducted over computer networks.

There is thus a need in the art for systems that undeniably put individuals or entities in control of the information regarding the transactions they conduct and the items that concern these transactions, in order to provide privacy, integrity, credentialing and security.

SUMMARY OF THE INVENTION

It is the object of the present invention to provide apparatus and methods that allow consumers, small businesses and corporations alike to implement processes and enforce policies allowing them to control and manage the privacy, integrity, credentialing and security of all objects, transactions, documents, entities and other items related to the execution of the transactions and the maintenance of electronic records regarding the items involved in these transactions. The invention is needed in the field of electronic commerce, order fulfillment, groupware and the like.

The invention includes:

A computer or computerized device (server, desktop, laptop, personal digital assistant, digital telephone) equipped with a biometrics measuring device, connected to it by secure communication means, whether wired or wireless and with software code permitting biometric authentication, symmetric or asymmetric encryption and decryption, middleware to manage secure communication, secrets databases, access control, key management license modules.

When a consumer contacts a web portal with the purpose of conducting electronic business transactions, the consumer uses the PICS system as follows:

Access the portal, by establishing a secure pipe on the network or world wide web,

Transmit a software agent to the portal inviting the portal to conduct business with the consumer,

An operator entitled to do so at the portal attaches a certificate to the plug–in,

The certificate contains an order form, and a price quotation, and is hashed. The hash, and the hash key are encrypted with the private key of the sales operator and transmitted to the consumer, who decrypts it with the public key of the operator according to the usual procedures known in the art.

The consumer then fills out the order form, hashes it attaches an electronic signature including an identity and a proof of signature verification, and transmits that message over the secure pipe to the sales operator, who sends in a similar manner a sales acceptance notification.

All information is stored in the secrets databases of the transacting parties.

As a result the personal privacy and the data integrity of the credentialed consumer is kept secure, while the portal can use statistical evidence and non-private information. The occurrence of the transaction cannot be repudiated. If there is a need to verify the content of the data, both parties must participate in order to make it possible to fully decrypt the data to a clear message.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates the apparatus.

FIG. 2 describes functional block diagrams.

DESCRIPTION OF AN ILLUSTRATIVE EMBODIMENT OF THE INVENTION

The foregoing brief description as well as further objects, features, and advantages of the present invention will be understood more completely from the following detailed description of the illustrative embodiments of the invention, with reference to the accompanying drawings, in which:

A Biometrics Measurement Apparatus (**1101,1102,1103,1104**) produces a dynamic biometric signature (**1110**) of a buyer (**1000**).

The buyer has registered a Signature Template (**1001**), it is encrypted and stored securely in an secrets database(**1200**), that contains the Signer ID, the Signature-Template (**1002**)and optionally other data like an authorization entitlement and private RSA key for use with a PKI.

When the Biometrics Measurement Apparatus (BMA, **1100**) is activated, a Transaction Security Module (**1300**) creates a session key(**1310**). The session key (**1310**) is kept in the secrets database(**1200**).

The session key combined with the identification number(1101) of the BMA(1100) is used to encrypt the biometric signature data (BSD) (**1110**). Asymmetric encryption can be used with RSA keys, or symmetric encryption can be used with AES standard keys. Verification of the BSD (**1110**) with the template (**1002**) if positive results in a Positive Signature Verification Message (**1300**). It is signed with the user's RSA key, and thus secure and unchangeable, guaranteeing the integrity of the information. Alternatively strong symmetric encryption can be used. If negative, an exception handling occurs alerting the buyer of an attempt at tampering or other unusual behavior of the BMA.

The buyer pushes, as known in the art, a software agent (**1400**) such as an applet, to the seller's (**2000**) portal (**2100**). This opens a secured pipe (**4000**) as known in the art.

The buyer sends a hashed request for proposal (RFP) (**1500**) together with the PSV (**1300**) to the seller over said secured pipe (**4000**). When the sales portal (**2100**) receives the PSV (**1300**) secured RFP (**1500**), an authorized sales person sends a standard X509 certificate (**2001**) to the buyer (**1000**), upon which

the buyer (**1000**) returns a standard (MD5, SHA1) hash key (**1600**), over said secure pipe (**4000**). The seller (**2000**) uses the hash key to reconstruct the RFP (**1500**). The seller (**2000**) than creates a proposal (**2700**), signs it digitally with a private key (**2002**), attaches a public key (**2003**), and hashes the message with said hash key (**1600**). Then the seller (**2000**) transmits the message over said secure pipe (**4000**) to the buyer (**1000**). A MAC guarantees the message integrity, as known in the art. The MAC is stored in the buyer's secrets database (**1200**). This is also done at the seller's (**2000**) secrets database (**2200**).

In similar ways, upon acceptance of the proposal (**2700**), the buyer sends an electronically signed purchase order (**1710**) to the seller(**2000**), who returns an electronically signed sales agreement(**2710**). Alternatively these transactions may be linked to third party information systems (**3000**), such as the buyer's electronic banking system (**3100**), or the sellers order fulfillment system (**3200**). Upon termination of the transaction the software agent (**1400**) removes all traces of the transaction from the sellers (**2000**) website (**2100**), with the exception of the information stored in the seller's secrets database (**2200**), and the secured pipe (4000) is closed.

Since all items related to the transaction are stored in the secrets database (**1200, 2200**) of both buyer (**1000**) and seller (**2000**), all transactions are traceable. Information maybe reconstructed with guaranteed integrity, when required. Private information may only be made "clear" with permission of both seller and buyer and always under the control of the buyer, since the buyer is the keeper of the session key (**1310**), required to regenerate the original authorization to start the transaction.

Neither the seller nor the buyer can repudiate the transaction, since both appended electronic signatures to the transaction records. Because all the information is hashed when stored, no changes can be made to it and that guarantees the integrity of the transaction records. The content of the secrets databases can only be revealed when buyer and seller agree and exchange the necessary encryption keys. That warrants the confidentiality of the transaction data, without restricting the usage of the data for statistical purposes.

Key management and key loading is the responsibility of the transacting parties (**1000,2000**). They can request supervision from Trusted Third Parties (**3000**).

5

Although preferred embodiments of the invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that many additions, modifications, and substitutions are possible without departing from the scope or spirit of the invention as described above.

What is claimed is the following:

1. A method for secure peer-to-peer electronic commerce.

2. The method of claim 1 whereby biometric means assure the positive proof of participation of individuals.

3. The method of claim 2 whereby the privacy of the participating individuals is assured.

4. The method of claim 3 thereby assuring the integrity of the data resulting of the transaction.

5. The method of claim 4 thereby relying on credentialing to determine the entitlement of the individuals involved in the electronic transaction.

6. The method of claim 1 whereby asymmetric encryption is used in an open Public Key Infrastructure.

7. The method of claim 1 whereby symmetric encryption is used in a private closed infrastructure.

8. The method of claim 6 whereby the certificate used in the Public Key Infrastructure belongs to a single portal and is complemented with the biometrics and credentialing of the participating individuals to generate unique instances of derived certificates, whereby the participants in the transaction do not require a separate certificate thanks to the method of claim 2.

FIG. 1

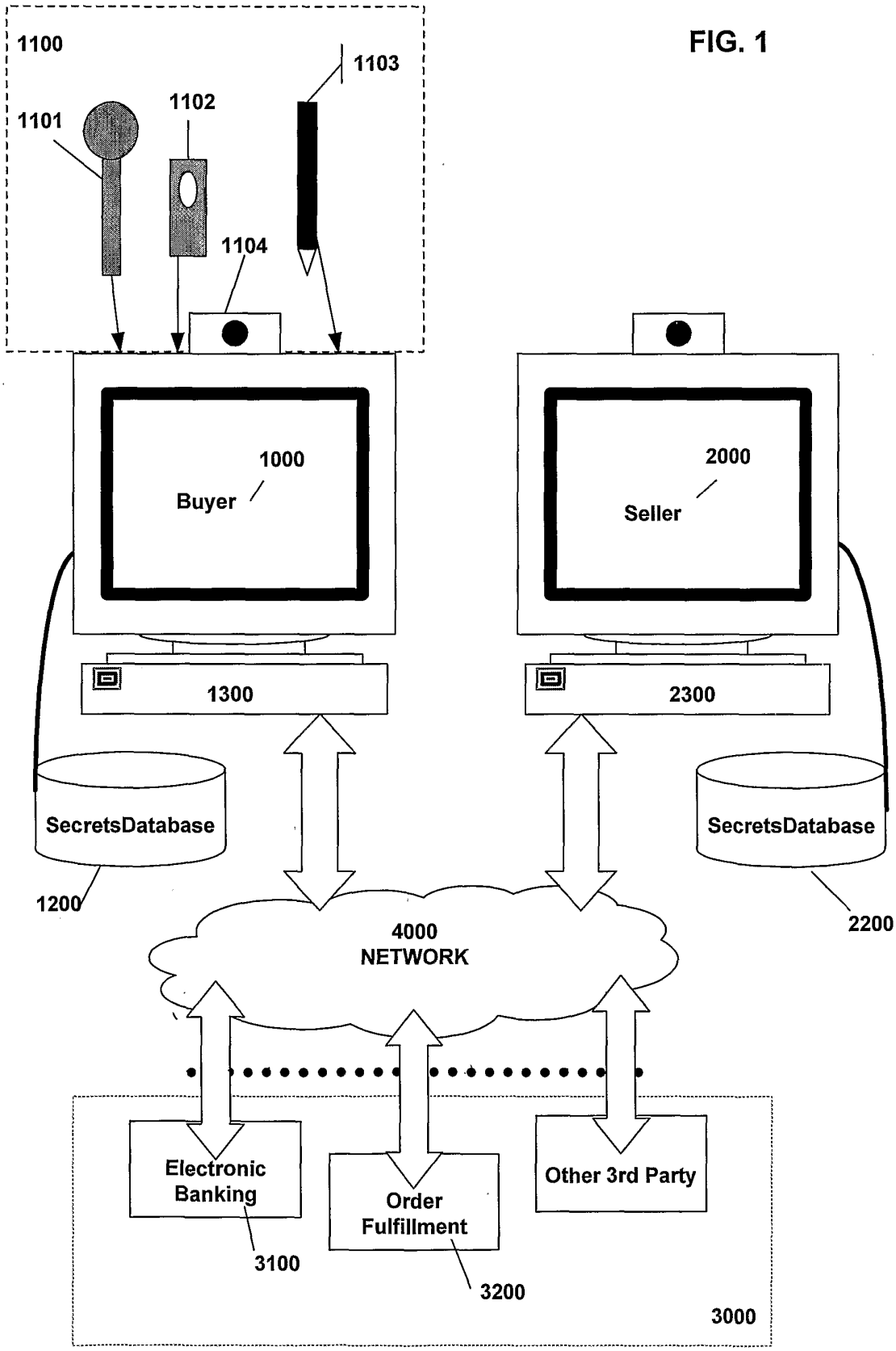

1100
1101
1102
1103
1104
1000
Buyer
2000
Seller
1300
2300
SecretsDatabase
1200
SecretsDatabase
2200
4000
NETWORK
Electronic Banking
3100
Order Fulfillment
3200
Other 3rd Party
3000

FIG. 2

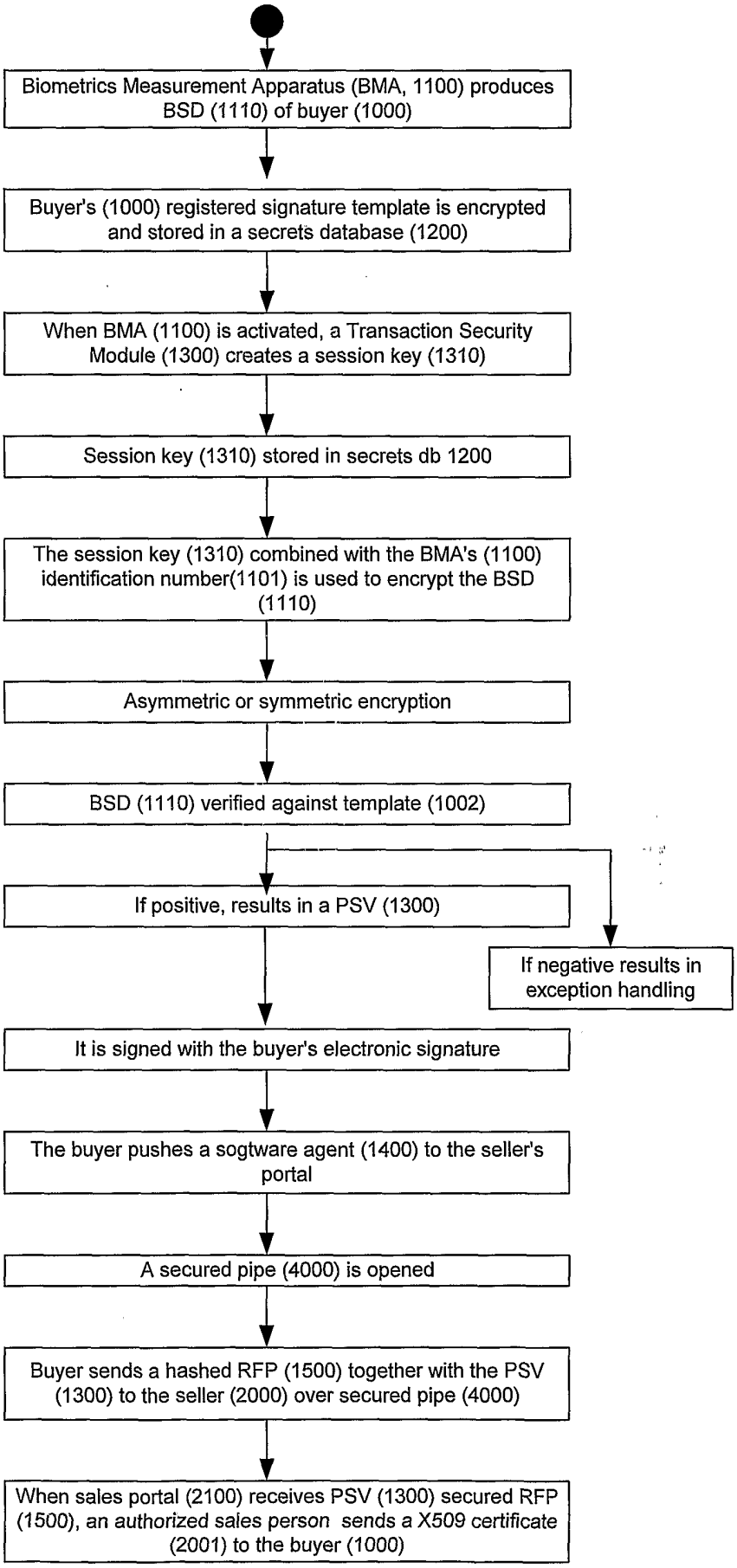
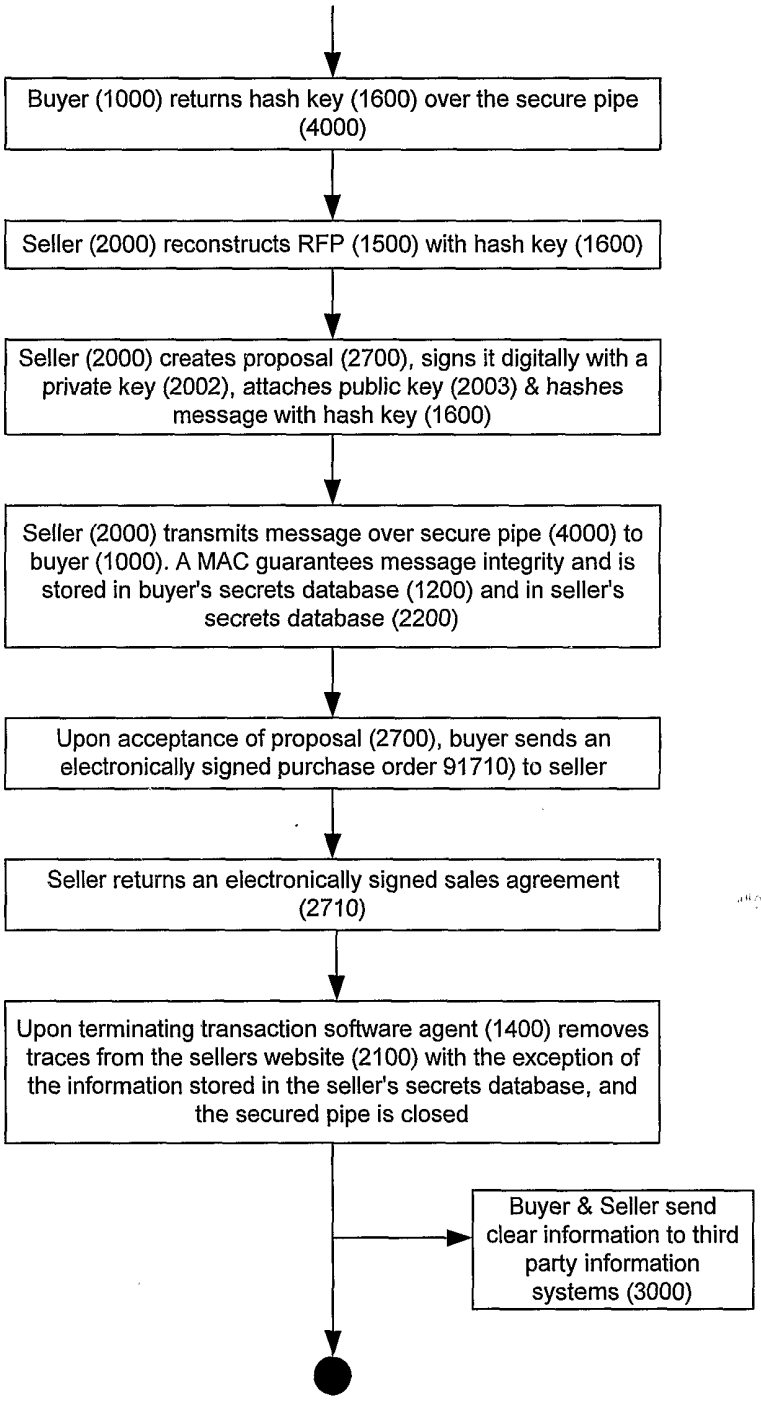

Biometrics Measurement Apparatus (BMA, 1100) produces BSD (1110) of buyer (1000)
Buyer's (1000) registered signature template is encrypted and stored in a secrets database (1200)
When BMA (1100) is activated, a Transaction Security Module (1300) creates a session key (1310)
Session key (1310) stored in secrets db 1200
The session key (1310) combined with the BMA's (1100) identification number(1101) is used to encrypt the BSD (1110)
Asymmetric or symmetric encryption
BSD (1110) verified against template (1002)
If positive, results in a PSV (1300)
If negative results in exception handling
It is signed with the buyer's electronic signature
The buyer pushes a sogtware agent (1400) to the seller's portal
A secured pipe (4000) is opened
Buyer sends a hashed RFP (1500) together with the PSV (1300) to the seller (2000) over secured pipe (4000)
When sales portal (2100) receives PSV (1300) secured RFP (1500), an authorized sales person sends a X509 certificate (2001) to the buyer (1000)

FIG. 2 Cont.


Buyer (1000) returns hash key (1600) over the secure pipe (4000)
Seller (2000) reconstructs RFP (1500) with hash key (1600)
Seller (2000) creates proposal (2700), signs it digitally with a private key (2002), attaches public key (2003) & hashes message with hash key (1600)
Seller (2000) transmits message over secure pipe (4000) to buyer (1000). A MAC guarantees message integrity and is stored in buyer's secrets database (1200) and in seller's secrets database (2200)
Upon acceptance of proposal (2700), buyer sends an electronically signed purchase order 91710) to seller
Seller returns an electronically signed sales agreement (2710)
Upon terminating transaction software agent (1400) removes traces from the sellers website (2100) with the exception of the information stored in the seller's secrets database, and the secured pipe is closed
Buyer & Seller send clear information to third party information systems (3000)