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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 September 2002 (26.09.2002)

PCT

(10) International Publication Number
WO 02/075616 A1

(51) International Patent Classification[7]: G06F 17/60, G06K 19/07

(21) International Application Number: PCT/AU02/00317

(22) International Filing Date: 20 March 2002 (20.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PR 3845 20 March 2001 (20.03.2001) AU

(71) Applicant *(for all designated States except US)*: **THE DEPARTMENT OF NATURAL RESOURCES AND ENVIRONMENT FOR AND ON BEHALF OF THE CROWN IN RIGHT OF THE STATE OF VICTORIA** [AU/AU]; 8 Nicholson Street, East Melbourne, Victoria 3002 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **BARRY, John, Patrick** [AU/AU]; 17 Greenslopes Drive, Carrum Downs, Victoria 3201 (AU).

(74) Agent: **GRIFFITH HACK**; 509 St Kilda Road, Melbourne, Victoria 3004 (AU).

(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:
— *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.

WO 02/075616 A1

(54) Title: IDENTIFICATION AND AUTHENTICATION DEVICE

(57) Abstract: The invention provides an identification and authentication device for a user to identify himself or herself and to execute documents or transactions, comprising: identification means for identifying the user; transaction authority means, for indicating the type or types of transaction that the user can execute by means of the device; and digital storage capacity; wherein the device is operable to identify the user, and by the user to execute transactions of the type or types specified by the transaction authority means.

IDENTIFICATION AND AUTHENTICATION DEVICE

FIELD OF THE INVENTION

The present invention relates to an identification and authentication device, of particular but by no means exclusive application in electronic transactions involving one or more parties and to electronic conveyancing. In the following description, it will be understood that references to "goods and services" or "goods or services" should be interpreted broadly, and to include all vendible items including property (including real and intellectual property) such as parcels of land or parts thereof. Further, although the present invention will be described in the context of land conveyancing, it will be understood by those in the art that it is of broad application, including in the areas referred to above.

BACKGROUND OF THE INVENTION

Land conveyancing is a common multi-party transaction, commonly involving - in addition to the vendor and the purchaser - a regulatory authority (such as a Lands Department or the like), a first financial institution (to which the vendor has mortgaged the property) and a second financial institution (to which the purchaser will mortgage the property). Existing methods for land conveyancing - and for conducting other multi-party transactions - generally follow the traditional approach in which the required documents are executed by the respective parties, and those documents, together with payments in the form of cash or cheque and possibly a title document (e.g. a land title), are exchanged. The transaction may also be recorded, as required, with one or more interested authorities.

In some such methods some of the steps described above are replaced by their electronic analogue. For example, payment may be exchanged electronically.

In the particular example of existing paper based land conveyancing, there are commonly six steps in a standard transaction comprising a residential sale and purchase. At each step, the information required is gathered anew, collected in appropriate forms and executed. Then, these forms are put aside and the parties proceed to gather the very same sort of information for the next step in the transaction.

Almost at the end of the transaction (or settlement), the final set of forms executed by the parties are exchanged by the vendor in return for the payment of money first to discharge any outstanding mortgage and secondly to pay the balance to the vendor. This requires settlement clerks for all sides to attend personally and make the exchange.

At the very end of the transaction, the purchaser (or the purchaser's mortgagee if the purchaser has sought finance with which to buy the property) commonly attends a Land Registry and lodges the forms signed by all parties for registration.

Once registration occurs, the interest is passed by law from the vendor to the purchaser. Until that time, the purchaser holds only an equitable interest in the land, an interest vulnerable to easy defeat by a competing interest.

Most of the information provided in the forms lodged with the Land Registry for registration originated with Land Registry. The need to transcribe this information to forms for registration results in substantial errors and mistakes as well as being impractical.

The other characteristic of current paper based conveyancing processes is that a vendor must prove to a purchaser that the vendor has the right to sell the land. This proof of a vendor's entitlement to sell is passed at

settlement to the purchaser and if there is a purchaser's mortgagee, to the purchaser's mortgagee. Without this proof of a vendor's entitlement to sell the land, the Land Registry will not register the interest of the incoming purchaser or purchaser's mortgagee.

Currently, this proof of a vendor's entitlement to sell is usually a Certificate of Title in the name of the vendor for the land being sold. The Certificate of Title is a (generally) partial copy of the original records held by Land Registry. Where the Certificate of Title is in the name of the vendor, there is a presumption that vendor is the registered proprietor of the land and hence entitled to sell it.

Where a registered proprietor has died or is no longer competent to dispose of his or her property, the proof of the vendor's right to sell may be not only the Certificate of Title in the name of the proprietor but supporting documentation that demonstrates how the vendor is able to sell the land. This may be by means of a grant of Probate of the Will (or equivalent) of the registered proprietor showing the vendor as the executor of the proprietor. It may perhaps be an order made by a Guardianship and Administration Board entitling the vendor to sell as the administrator of the registered proprietor.

Whatever the proof of the vendor's right to sell the land, that proof has to be passed to the purchaser or the purchaser's mortgagee at the time of settlement. Failure to do so means that the interest of the purchaser and purchaser's mortgagee will not be registered.

It will be clear that all the above techniques, and especially the existing paper based conveyancing process, remained constrained by the use of centuries-old step-by-step approaches, even where the most recent information and telecommunications are employed. Information is

commonly supplied by the very authority to which it will ultimately be lodged; a purchaser does not acquire a legal interest until some time after acquiring an equitable interest, and that equitable interest does not ensure that the legal interest will follow. The time required to complete such a transaction is altered little by the use of modern information systems, and this approach is still as vulnerable to the delays and bottle-necks that can arise from, for example, a party's delaying their execution of a document, or the failure of a party (or that party's representative) to attend a settlement meeting.

One existing attempt to proving an electronic conveyancing system is disclosed in WO 00/55774 (Bolero International Limited). This document discloses a centralized database system for supporting transactions in property, accessible by users over - for example - the internet. The central database forms a title registry recording the entitlements of the users to perform specified actions in relation to electronically created records that represent a defined series of rights and obligations in relation to underlying property. The users become entitled by virtue of their designation to prescribed roles by a previously entitled user. Designation of a user to a prescribed role in a record takes place by means of a system user sending an electronic instruction to the database, these electronic instructions being referred to as registry instructions or title registry instructions.

However, this system is limited to a transaction support system with a central registry database, and a secure message handling facility so that users can create, maintain or deactivate records stored in that database. The system also includes a "registry maintenance unit" to mediate between the registry database and the message system. As such there is little to distinguish this system from existing paper-based systems beyond a

straightforward translation to the internet of older approaches.

An electronic trading system is disclosed in US Patent No. 5,717,989 (Full Service Trade System). A system stores criteria specified by a funder relating to trade transactions for buyers and sellers, then compares the criteria with a proposed purchase order to determine whether the system can generate a payment guarantee on behalf of the funder for the buyer to the seller. The system also compares subsequent documents relating to an original purchase order with the original purchase order to ensure that the terms of the purchase order are properly fulfilled. When the appropriate conditions for payment are met, the system issues a funds transfer instruction to transfer payment from the buyer to the seller.

This system is intended to avoid the use of letters of credit and the manual processing of documentation but, in common with the system of WO 00/55774, is restricted to the use of a "data processing system" for receiving and comparing proposed contract data from a buyer and a seller. A contract is then deemed to have been established on the basis of the seller for payment under the contract.

Both of these systems (which are not suggested to form a part of the common general knowledge) merely appear to envisage, in effect, the replacement of a letter of credit or a bill of lading with a central database on which is stored all the information that would be, in paper-based prior art systems, included in such documents.

SUMMARY OF THE INVENTION

In a broad aspect, therefore, the present invention provides an identification and authentication device for a user to identify himself or herself and to execute

documents or transactions, comprising:

identification means for identifying said user;

transaction authority means, for indicating the type or types of transaction that said user can execute by means of said device; and

digital storage capacity;

wherein said device is operable to identify said user, and by said user to execute transactions of the type or types specified by said transaction authority means.

Thus, the device - which would be provided upon presentation of suitable identification (e.g. passport, driver's licence, etc.) - enables the user to execute transactions, but only of types specified by the transaction authority means of the device. This mechanism can be used to avoid conflicts of interest.

Preferably said transaction authority means comprises transaction authority information stored in said digital storage capacity.

The digital storage capacity may comprise a computer disk drive or merely a surface of the device bearing the relevant information in bar code or other comparable format.

Preferably said device is operable to expire after a predetermined period.

Thus, the device can be programmed to no longer provide identification or to execute transactions after a period (determined and fixed at issue of the device) has elapsed.

Preferably said identification means is stored in said digital storage capacity.

Preferably said device is operable to download and store (preferably in said digital storage capacity) data

pertaining to said documents or transaction.

Thus, the device may be used to check details of a transaction, and the results of that check can then advantageously be stored in the device.

Preferably said device is operable to store details of an electronic financial instrument associated with said transaction.

Thus, payment associated with said transaction can be facilitated by means of the device.

Preferably said transaction authority means is operable to authorize a predetermined type or types of transaction only when a password has been provided to said device or in association with said transaction.

Preferably said transaction authority means designates that said device is for use by a vendor or member of a group who owns, controls or possesses the title to goods or services where goods include any rights in land. Alternatively, said transaction authority means designates that said device is for use by a purchaser or a member of another discrete group. Alternatively, said transaction authority means designates that said device is for use by an agent of another party whether or not this user is an agent of the said groups.

Preferably, when said transaction authority means designates that said device is for use by a vendor or member of a group who owns, controls or possesses the title to goods or services where goods includes any rights in land, said device is operable to retain information pertaining to that which said vendor or member of said group intends to sell assign, lease or otherwise limit his or her right to said goods or services. More preferably, the device is provided with this information when the

device is issued only.

Thus, the vendor or member of a group who owns, controls or possesses the title to goods or services where good includes any rights in land might specify a particular parcel of land he or she wishes to sell, assign, lease or otherwise limit his or her right to said goods or services. In a preferred form, the device is then specific to that combination of goods or services and vendor or said member.

Preferably said device is a computer peripheral device operable to communicate digitally with a user computer (whether connected by cable, infra-red or otherwise).

Preferably said identification and authentication device has a secondary operating system and is operable to load digital data into a user computer having an input means and an operating system, by:

arranging said user computer and said identification and authentication device to be in data communication with one another;

transferring said secondary operating system from said identification and authentication device to said user computer;

running said secondary operating system on said user computer such that control of said input means is appropriated by said secondary operating system; and

mediating at least some communication between said user computer and said identification and authentication device by means of said secondary operating system;

whereby said at least some communication is performed other than by means of said operating system of said user computer.

Preferably said identification and authentication device is operable to process digital data located on said

identification and authentication device, whereby said processed digital data is subsequently transferred to said user computer, and said processing of said digital data is performed by said identification and authentication device rather than by said operating system of said user computer.

Thus, the digital data can be processed within the identification and authentication device before being seen by the operating system of the user computer, so such processing can be done without the involvement of the operating system of the user computer.

Preferably said user computer is operable to receive said digital data by means of said input means after said secondary operating system has appropriated control of said input means, whereby said digital data is subsequently transferred to said identification and authentication device.

Thus, the digital data to be loaded into the user computer may originate in the identification and authentication device, or firstly be entered by means of the input means of the user computer and then transferred to the identification and authentication device.

Preferably said secondary operating system is operable to create a memory space within said user computer to gain control of said input means (such as a keyboard).

Preferably said secondary operating system is operable to mediate input of a password or passphrase, to pass said password or passphrase to said identification and authentication device, and to process said digital data according to said password or passphrase. More preferably said secondary operating system is operable to employ said password or passphrase to encrypt or decrypt some or all of said digital data

Preferably said processing of said digital data comprises manipulating said digital data, screening said digital data or both manipulating and screening said digital data. Manipulating said digital data may comprise encoding said digital data, while screening said digital data may comprise checking said digital data for viruses.

Preferably said identification and authentication device is a computer peripheral device operable to communicate digitally with said computing device (whether connected by cable, infra-red or otherwise).

In a second broad aspect, the present invention provides an electronic transaction system for conducting a transaction over a computer network, comprising:

submission means for allowing any of one or more users to submit respective user information pertaining to said transaction, the sum of said respective user information at any time constituting transaction information;

storage means for storing and retrieving said information; and

execution means in the form of an identification and authentication device as described above, for allowing any of said users to execute or indicate assent to at least some of said transaction information;

wherein said transaction information, when complete, includes all information required to conduct said transaction, and whereby any of said users can submit, inspect and execute or assent to any part of said transaction information required for said transaction to be completed.

Thus, the electronic transaction system does not itself impose a limit on the number of parties that could be involved in the transaction as, although the system could be implemented on a single server, there is not reason in

principle why each user could not use his or her own computer for storing their own user information, or for running some of the programs needed to operate the system.

The submission means may comprise software portions, software portions stored on a computer readable medium, computer hardware, or a combination of hardware and software. The same is true for the storage means and the execution means. Further, each of these means may comprise a single, discrete means (such as a central program running on a remotely accessible server), or downloadable software so that each user has a local copy of such software. In such an arrangement, therefore, the submission means could comprise the sum of all the software copies used by all the parties to the transaction.

Preferably said system includes means for retrieving, or for retrieving and displaying, said transaction information to any of said users. More preferably said system includes means for retrieving, or for retrieving and displaying, said transaction information to any of said users in a single coherent form, whereby said transaction information appears to comprise a single document or computer file.

Thus, a user need not be aware that the transaction information has been collected from one or from many locations; the system will present the transaction information to the user as though retrieved from a central database, whether or not this is so.

Preferably the storage means comprises software portions for controlling the storage and retrieval of the respective user information. Alternatively, the system may include one or more computer readable and writeable media for storing the respective user information, in which case the storage means may comprise software

portions for controlling the storage and retrieval of the respective user information and said one or more computer readable and writeable media.

The one or more computer readable and writeable media preferably comprise a plurality of computer storage devices (such as hard disks) and specifiable by each of said respective users, whereby each of said respective users can specify which of said plurality of computer storage devices is to be used for storing said respective user information of said respective user.

Preferably said system includes pointer storage means for the storage of information storage pointers, whereby said system is operable to maintain in said pointer storage means a pointer to the location of each item of user information stored by said storage means.

Thus, the pointer storage means (typically a database) does not have to store any of the user (or thereby transaction) information. Rather, the system maintains in the pointer storage means a record of where that information is stored. Consequently, the system need not itself include computer storage devices for storing the user information; these could be the users' own computer disks (although such disks could validly be regarded as a part of the system). The system keeps a record of where the information has been stored so that that information can be stored and retrieved when needed.

Preferably said system includes an electronic financial instrument, comprising:

digital data packets encoding information concerning one or more payments pertaining to a transaction;

digital storage means for storing some or all of said data packets; and

display means for displaying some or all of said

information.

For example, if - in a conventional paper-based transaction - there were a cheque from A to B, a second cheque from C to D and a third cheque from E to F, according to the present invention these three cheques would be replaced by a single electronic instrument.

For example, if - in a conventional paper-based transaction - there was partial title to good and services held by X, partial title to the same goods and services held by Y and a third partial title to the same goods and services held by Z, according to the present invention, the three partial titles to goods and services would be replaced by a single electronic instrument.

For example, if - in a conventional paper-based transaction - there was title to some goods or services held by P, title to the other goods or services held by Q and a third title to still other goods or services held by S, according to the present invention, the three titles to different goods or services would be replaced by a single electronic instrument.

Preferably said instrument is operable to display said information to a user only upon presentation by said user of suitable identification.

More preferably said instrument is operable to display to said user only that part of said information pertaining to said user.

Thus, the user may be shown only what he or she is required to pay, assign, lease or otherwise limit his or her right to said goods or services to other parties, and what he or he should expect to receive from others parties, even though the overall transaction may include the exchange of consideration between those other parties.

Still more preferably, said instrument is operable to display to said user only that a summary of said information in which net payments or obligations to or from said user are indicated.

Thus, a user who is entitled to receive funds will only be able to access details of the funds to which he or she is entitled. In the above example of the three cheques, the total obligation of A is contained in his or her promise to pay B. According to the present invention, in that example, the total obligation of A may be greater that his or her obligation to B. It may be part of the obligation to C. Similarly, the obligation of E might be less than any total payment due to F. In other words, the total amount of the obligations of the payees equal the payments due to the recipients but there is no necessary correlation between the individual obligations of a payee and payments due to any individual.

In the above example of the three partial titles to the same goods or services, the total ownership of X is contained in his or her partial title to goods or services. According to the present invention, in that example, the ownership of X may be less than the total ownership in the goods or services. The payment due to him or her from any person or persons purchasing title to the total goods or services may be proportionately lesser or greater than his or her proportionate title to the goods or services. Similarly with Y and Z. In other words, the total amount of the obligations of the payees or the total title to the goods or services held by X, Y and Z is equal to the payments due to them but there is no necessary correlation between the individual obligation of the payees or their total title to goods or services and the payments due to X, Y and Z.

In the above example of the title to the three sets of

different goods or services, the total ownership of Q is contained in his or her title to goods or services. According to the present invention, in that example, the ownership of Q is less than the total ownership in the goods or services conveyed. The payment due to him or her from any person or persons purchasing title to the total goods or services may be proportionately lesser or greater than his or her proportionate title to the goods or services. Similarly with P and S. In other words, the total amount of the obligations of the payees or the total title to the goods or services held by P, Q and S is equal to the payments due to them but there is no necessary correlation between the individual obligation of the payees or their total title to goods or services and the payments due to P, Q and S.

Similarly, a user who is required to provide title, whether full or partial, to goods or services will only be able to access details of the title to goods or services which he or she is entitled

Preferably said electronic instrument is a financial instrument including but not limited to bill of lading, insurance bond, bearer bond, banker's warrant and capable of being negotiated , and more preferably operable to function as an electronic bank receipt.

Preferably said instrument is storable on a portable device, more preferably on said identification and authentication device.

Preferably said system includes a secure data management method means, comprising:

retrieval means for retrieving information pertaining to a transaction from one or more digital storage means;

inspection means for inspecting said information to determine whether said information includes or has been

associated with suitable ratification data indicative of the ratification of said information or respective parts of said information by respective parties to said transaction; and

ratification means for flagging said transaction as ready for settlement if said ratification data is located.

Preferably said transaction settlement means is operable to deem said transaction as ready for settlement at a predetermined time.

Thus, the parties may agree that settlement will occur at a specific date and time after all parties have ratified their part of the transaction details.

Preferably said inspection means comprises computing means, and more preferably a server connected to the internet but accessible for said transaction by said parties.

Preferably said digital storage means is not a part of said computing means. Thus, the computing means preferably acts merely as a gateway.

Preferably said system is operable:

by a respective party or a user who has not submitted user information to a transaction to copy information pertaining to said party or any information to which said user has access and to said transaction from a computer network onto a user computer of said party or a user who has not submitted user information;

by said party or a user who has not submitted user information to augment or amend said downloaded information to form amended information;

by said party or a user who has not submitted user information to execute or assent to said amended information so that said amended information includes

execution data; and

to compare said amended information with said information and deem those parts of said amended information that are consistent with said information to have been executed or assented to.

Thus, a party to a transaction need not conduct their part of the transaction online, but can work on a copy or clone of the details relevant to them on a local computer.

Preferably said system is operable to augment said downloaded information with the time of downloading.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the present invention may be more easily ascertained, an embodiment will now be described by way of example with reference to the accompanying drawings, in which:

Figure 1A is a flow chart of an electronic conveyancing system according to an embodiment of the present invention;

Figure 1B is a schema of the system architecture underlying the electronic conveyancing system of figure 1A and its interrelationships up to the time of settlement;

Figure 1C is a schema the system architecture underlying the electronic conveyancing system of figure 1A and its interrelationships during and after the time of settlement;

Figure 2 is a pre-settlement flow chart of the Land Trader transaction engine of the electronic conveyancing system of figure 1A;

Figure 3 is a post-settlement flow chart of the Land Trader transaction engine of the electronic conveyancing system of figure 1A;

Figure 4 is a schematic representation of the hardware components of the Land Trader transaction engine of figures 2 and 3;

Figure 5 is a flow chart of the data traffic from

the Land Trader transaction engine to the user-side storage plugs of the electronic conveyancing system of figure 1A;

Figure 6 is a flow chart of the data traffic from the Land Trader transaction engine to the transaction storage plugs of the electronic conveyancing system of figure 1A;

Figure 7 is a schematic representation of a cover sheet of the electronic conveyancing system of figure 1A;

Figure 8 is a schematic representation of a Land Card of the electronic conveyancing system of figure 1A;

Figures 9A and 9B depict a flow chart of the data traffic during the first entry of data into the Land Card of figure 8;

Figures 10A and 10B depict a flow chart of the data traffic during the second and subsequent entry of data into the Land Card of figure 8;

Figures 11A, 11B and 11C depict a flow chart of the data traffic associated with the Land Card of figure 8 during settlement;

Figure 12 is a flow chart of the data traffic associated with the use of the Land Card of figure 8 with a financial instrument in the form of an electronic bank receipt;

Figures 13A, 13B, 13C and 13D depict a flow chart of the settlement process of the electronic conveyancing system of figure 1A during settlement;

Figures 14A and 14B depict a flow chart of the locked file of the electronic conveyancing system of figure 1A;

Figures 15A, 15B and 15C depict a flow chart of the data traffic associated with electronic transfer of funds by means of the electronic conveyancing system of figure 1A;

Figures 16A and 16B is a flow chart of the data traffic associated with the negotiation of an electronic bank receipt by means of the electronic conveyancing system of figure 1A;

Figure 17 is a schema of the parasitic operating system of the Land Card of figure 8 and its relationship to the Land Card and the user computer; and

Figure 18 is a flow chart of the operation of the parasitic operating system of figure 17.

Figure 19 is a schema of the operation of the presentation and transport layers and their toolboxes.

DETAILED DESCRIPTION OF THE INVENTION

A flow chart of a secure data management system in the form of an electronic conveyancing system incorporating an identification and authentication device according to a preferred embodiment of the present invention is shown in figure 1A.

OVERVIEW

The present is described in the context of a secure data management system in the form of an electronic conveyancing system that enables one or more users to enter their own unique data in the system in a way that preserves their control over the storage and access to their data.

Unlike most data management systems, this secure data management system does not track and manage data on the basis of individual data packets or on the basis of data packets aggregated as notional "documents". Instead, it views every piece of data as being part of a transaction in which one or more users are taking part. In any transaction, some data is needed by all users in the transaction. This can be as basic as the parties' names and addresses and a number common to the parties, such as found on an invoice. Rather than tracking and managing this data that is reused again and again, this secure data management system manages the transaction as a whole.

This ensures that the secure data management system can

manage the transaction at various stages of its life and accommodate partially complete data elements as the inevitable negotiations that form part of most transactions.

The secure data management system is capable of a multi-lateral operation. This ensures that it can be used not only for managing the data of a single entity but is capable of accommodating transactions with multiple parties.

Because of the importance of role based access controls and because access to data is controlled by those who provide the original data, a single secure data management system can be used across safely and confidently across corporate boundaries without risk to the data of any individual or each corporate entity using the secure data management system.

Central to the secure data management system is the concept of an independent verification of the identity of all users. This ensures that the secure data management system offers users the very high confidence when dealing with otherwise unknown users. The secure data management system also offers users the confidence that any fraudulent attempt to repudiate a transaction or any data provided as part of the transaction can be detected and prosecuted.

Where financial payments are involved, the secure data management system ensures that users can be confident that all financial payments will be honoured and no financial payments will be made without the certainty of receiving goods or services bargained for. In this area, the secure data management system also offers users the confidence that payments and title to goods will pass together at the same time.

Finally, where transactions are subject to data being provided from other systems, the secure data management system offers a means of delivering this data to a transaction in a way that ensures that the necessary data is incorporated into the transaction in a common useable and intelligent format. Where a user has paid for information from another system, he or she maintains her investment in the information. A user obtaining the data from other systems controls the data and can give access to it or parts of it to any other user.

The security of the secure data management system is maintained by multiple layers of security. However, even in the event that the system is breached, the potential loss to any user is minimized by two characteristics of the secure data management system. Firstly, the secure data management system only stores the location of data controlled by each of the users. The secure data management system does not store any record of the data itself nor does it store any details of what data is stored by each of the users. It does not control the data nor does it store the data from any transaction. The users themselves control the storage of the data.

If breach of the secure data management system were to occur, only the location of unknown data belonging to a series of users would be available for use, not the content of what that data is nor which user stores what data. Any person breaching the security of the secure data management system would then face the task of ascertaining which storage node stored which data as well as the task of breaching the security surrounding the secure storage sites in which the users' data was stored.

Secondly, all data stored by the secure data management system is asymmetrically encrypted by the user. The secure data management system does and cannot decrypt this data. Its task is to retrieve data from secure storage

sites and pass to a user for decryption and presentation.

At a more detailed level, the data entered by users or delivered at their request to the secure data management system is not stored by the secure data management system. Instead, the secure data management system transmits the users' data to a secure storage site chosen by the user. Only the details needed to locate and recover data from the secure storage site are stored by the secure data management system.

In some cases, users of the secure data management system can request other computer systems to which they are access to search for and deliver requested data to the secure data management system. Once the data from another system is delivered, the user who requested the data maintains control over the storage and access to this data.

When a user controlling the data wishes to inspect, retrieve or modify the data managed by the secure data management system, that user identifies himself or herself to the secure data management system. The secure data management system then uses the details of the data's location stored by it to retrieve the data held by the secure storage site and displays that data to the user controlling it in a common agreed format.

If no modification is made to the data, the secure data management system makes no change to the details of the data's location.

If the user controlling the data modifies the data, he or she authorizes the change and then commits it. Upon commitment of the change, the secure data management system transmits users' modified data to a secure storage site chosen by the user.

As well as the key necessary to access the secure data management system, the hardware token provided by an Identification Service Agency contains several other asymmetric keys. One of these keys, one half of the encryption keypair, is used by the hardware token to encrypt all data sent to secure storage by that user. Only data encrypted with that encryption key held in the hardware token issued to a user is sent to secure storage.

Only the details needed to locate and recover modified data from the secure storage site are stored by the secure data management system.

Where other users are given access to data by the user controlling that data, these other users granted may inspect, retrieve or modify the data to which they are granted access. The users given access to data identify themselves to the secure data management system and demonstrate their right of access to the data sought. The secure data management system then uses the details of the data's location stored by it to retrieve the data held by the secure storage site of the user controlling the data and displays that data in a common agreed format to the user granted access to the data.

If no modification is made to the data, the secure data management system makes no change to the details of the data's location. The data remains stored in the secure storage site of the user controlling that data.

If the user given access the data controlled by another user modifies that data, he or she authorizes the change to the data and then commits it. Upon commitment of the change, the secure data management system transmits the modified data to a secure storage site chosen by the user modifying the data. Only the details needed to locate and recover modified data from the secure storage site are stored by the secure data management system. The secure

data management system also transmits the date and time of the modification to the secure storage site of the user controlling the data to be added to the original data.

Where a user given access to data controlled by another user requests other computer systems to search for and deliver augmented or other data that pertains to the data to which he or she has been given access, the data from another system is delivered to the secure data management system. The secure data management system then transmits that augmented or other data to the secure storage chosen by the user who requested it. The user requesting the augmented or other data maintains control over the storage and access to this data but may give access to it to any other user.

Only the details needed to locate and recover augmented or other data from the secure storage site are stored by the secure data management system.

To ensure that access is restricted to the secure data management system and the data it manipulates, only users whose identity is verified may access the secure data management system. A user's identity is verified by an Identification Service Agency that satisfies itself that the evidence of the identification of a user is sufficient for it to issue a hardware token containing one half of an identification keypair to the user. Use of this half of the identification keypair verifies identification for that user.

On each occasion that a user enters the secure data management system, the secure data management system requires him or her to identify himself using the half of the identification keypair on the hardware token provided by an Identification Service Agency. The secure data management system then verifies that this verification of identification was issued by an Identification Service

Agency and remains valid and current.

If any part of this initial verification process fails when a user enters the secure data management system, the user is denied access to the secure data management system.

On first entry of a user into the secure data management system, the secure data management system requires the user to begin a specified transaction type or join a specified transaction.

If the user chooses to begin a specified transaction type, he or she is required to choose from a list of transaction types. Once this choice is made, the secure data management system allocates a unique number that the user will need on every other occasion that he or she wishes to view or modify data that the user controls or to which he or she has access for that transaction.

If the user chooses to begin a specified transaction type, he or she is then required to choose from a list of roles for the transaction type chosen. Once this choice is made, the secure data management system stores the unique number given to the transaction type that the user has chosen and stores the role chosen by the user against that transaction type for that user.

On every other occasion that a user wishes to view or modify data for that transaction, the user is required to adopt the same role for that transaction.

If, when entering the secure data management system for the first time, the user chooses to join a specified transaction, the secure data management system provides him or her with a list of transactions to which he has been given access by users controlling data in that transaction. The list of transactions also contains the

roles assigned to him or her for that transaction by users controlling data in that transaction.

In a limited number of cases, the user when choosing to join a specified transaction for the first time is offered a choice of roles in the transaction from those roles not yet chosen by other parties controlling data in the transaction.

In such case, the new user may choose any role from those not yet chosen by other parties.

In all cases, once a role is chosen, the secure data management system does not permit a user to change roles at any point in a transaction.

On every other occasion that a user enters the secure data management system, the secure data management system requires the user to begin a specified transaction type, join a specified transaction or continue a specified transaction. If, at the time the user enters the secure data management system, the user chooses to continue a specified transaction, the secure data management system will offer that user a choice to view or modify the data in any ongoing transaction in he or she has a role.

Where the user chooses to begin a specified transaction type or join a specified transaction, the secure data management system follows the same procedure as set out above.

Where the user chooses to begin a specified transaction type or join a specified transaction, the user is required to adopt the same role for that transaction on every other occasion that the user wishes to view or modify data for that transaction,

Where the user has a role in any ongoing transaction, the

secure data management system will permit him or her to view or modify data for that transaction. In such cases, the user will be required to adopt the same role for that transaction.

When users are authorized to have access to data or parts of the data by the users who control that data, the secure data management system displays that data in a common agreed format.

Every transaction has a completion time. Even a single party transaction, such as a file or document, is eventually complete and lodged in archival storage. The secure data management system requires that this completion for each transaction to be made explicit.

Before the completion time, the transaction must be ratified by the users who are party to the transaction.

Once a transaction is ready for completion, the secure data management system provides its elements to the users for ratification. The secure data management system distinguishes between a single party transaction and a transaction having more than one party in only one respect - that of the consequences of ratification where the transaction is a commercial one.

When a user in a single party transaction notifies the secure data management system is ready for completion, the secure data management system recalls all data from storage and presents it for decryption and ratification by the user. If the user is satisfied that the single party transaction is complete, that user uses one part of another asymmetric key pairs held in the hardware token by which he or she accesses the secure data management system to sign the ratification and so signal that he or she has completed the transaction. This is the ratification keypair, one half of which is held in the hardware token

issued to that user.

Where a single party transaction is not a commercial one, the secure data management system undertakes a series of "sanity" and software checks to ascertain that the transaction is complete and accurate and that the "snapshot" of the epitome (described below) has been validly ratified by a user who holds one of key pairs issued by an Identification Service Agency. In essence, the secure data management system ensures that the ratification has been undertaken by only a user whose identification key and ratification subkey remains valid and current.

Upon successful completion of these checks, the data in the epitome is then encrypted by the one half of the encryption key pair in the hardware token issued to that user by an Identification Service Agency and passed to the secure data management system. The secure data management system transmits the ratified "snapshot" to secure archival storage chosen by the user. It then notifies the user that the matter is complete.

Transactions within a corporate environment, such as a file or document, are often considered to be a single party transaction. This is misleading. These are usually multilateral transactions. Only because they are within the bounds of the corporate entity is it possible to consider them to be a single party transaction. Considered from the perspective of the secure data management system that is not limited by corporate boundaries, these types of transactions are multi party.

Multilateral transactions, that is, transactions that have more than one user involved in them at any stage of their life, are treated slightly differently. In all multilateral transactions, like single party transactions, there is an explicit completion time. Because

multilateral transactions have multiple parties, the completion time must be agreed by all users at the time that the transaction commenced.

Before the agreed completion time, each user in a multilateral transaction must ratify that part of the transaction that applies to him or her. When each user in a multilateral transaction is satisfied that his or her part in the transaction is complete, that user accesses the secure data management system by identifying himself or herself using the identification key in the hardware token issued by an Identification Service Agency.

That user then informs the secure data management system that he or she is ready to ratify the transaction.

Ratification in these circumstances is used deliberately in the secure data management system to avoid issues of asynchronicity associated with execution of documents or data. By using ratification, users can choose their own time to confirm or ratify their part of the transaction. They are not executing a component document or data packet but ratifying that part of the transaction as it applies to them. All users, however, must ratify the transaction before the agreed completion date.

This means, for example, that they might very well ratify the transaction at an earlier stage in the transaction, provided that they are satisfied that, upon completion, the completely ratified transaction will provide them with the goods or services expected of the transaction.

By notifying the secure data management system that he or she intends to ratify the transaction, the user enables the secure data management system to retrieve all data stored by that user in secure storage or to which that user has access. Using the location indicators and the access and role controls maintained by the secure data

management system, together with the access control of secure storage passed by this notification to the user, enables the secure data management system to retrieve all the data for the transaction that that user controls or which he or she has access.

All data for the transaction that that user controls or which he or she has access is transmitted by the secure data management system to that user, together with an template for the epitome for the particular transaction type that the user intends to ratify.

When decrypted by one half of a encryption key pair on the hardware token issued by an Identification Service Agency to that user, an epitome of the data is then presented to that user using the epitome template for that particular transaction type.

An epitome is a summary of the essentials of that particular transaction type that a user can examine and ratify. Part of the secure data management system is a presentation layer and presentation toolkit that enable templates for epitomes for transaction types to be prepared without programming skills.

In the case of transactions where there is no financial payments to be made, the epitome has the appearance of a summary of the data.

Using the one half of the ratification key pair on the hardware token issued by an Identification Service Agency to that user, each user ratifies the transaction by approving the epitome.

The ratification by each user results in the secure data management system taking a "snapshot" of the epitome that each user ratified.

Upon the last user who is party to the transaction ratifying the epitome and provided the ratification of each user remains in effect at the completion time, the settlement process for the transaction begins.

Where the transaction is not a commercial one, the secure data management system undertakes a series of "sanity" and software checks to ascertain that the transaction is complete and accurate and that all "snapshots" of the epitome has been validly ratified by users who hold one of ratification key pairs issued by an Identification Service Agency. In essence, the secure data management system ensures that the ratification has been undertaken only by users whose identification by an Identification Service Agency and whose ratification subkeys remains valid and current.

Upon successful completion of these checks, the "snapshots" of the epitome are then encrypted by the one half of the encryption key pair in the hardware token issued to each user by an Identification Service Agency and passed to the secure data management system. The secure data management system transmits the ratified "snapshots" to secure archival storage facilities chosen by the users. It then notifies the users that the matter is complete.

In some transactions, both single party and multilateral, another party may have an interest in the ratification. In a limited number of cases, another party may require details of the transaction to be filed or registered with it.

In cases where another party has an interest in the ratification and hence the completion of the transaction, the secure data management system is easily adapted, using its access and role controls, to ensure that it notifies the party interested that the matter is complete.

In cases where a party requires details of the transaction to be filed or registered with it, this too is dealt with using the access and role controls of the secure data management system. In such cases upon their completion, the secure data management system transmits a ratified series of "snapshots" of the epitome to secure storage chosen by that party.

These variations are dealt with by the transport layer inherent in the secure data management system. Part of the secure data management system is a transport layer and transport toolkit that enable such variations to be established or modified without programming skills.

Variations like this do require that a party receiving notification of completion or receiving "snapshots" of the epitome have its identification verified by an Identification Service Agency and a hardware token issued by it.

In the case of commercial transactions in which financial payments are to be made in return for goods and services, the epitome has the appearance of a balance sheet. In a bilateral transaction, one side of the epitome template shows payments to be made, together with the details of the payor and the payee and their banking details. The other side of the balance sheet shows goods and services to be delivered as a condition of the payments made.

In multilateral transactions in which financial payments are to be made in return for goods and services, the epitome is still in the form of a balance sheet but is more complicated because of the multiple parties to the transaction. One side of this balance sheet structure shows any payments to be received, together with the details of the payors and the payees and their banking details. It also shows goods and services to be delivered

as a condition of the payments made. The other side of the balance sheet shows payments to be received, together with the details of the payors and the payees and their banking details. It also shows goods and services to be received as a condition of the payments made.

Each epitome template is built using a presentation toolkit.

In these commercial transactions, ratification has different consequences. Before the agreed completion date, each user ratifies the transaction by approving the epitome. This is done using the one half of a ratification key pair on the hardware token issued by an Identification Service Agency to that user. The ratification of a user creates a "snapshot" of the epitome as ratified by that user.

Upon the last user who is party to the transaction ratifying the epitome and provided the ratification of each user remains in effect at the completion time, the settlement process for the transaction begins.

Where the transaction is a commercial one, the secure data management system undertakes a series of "sanity" and software checks to ascertain that the transaction is complete and accurate and that all "snapshots" of the epitome has been validly ratified by users who hold one of ratification key pairs issued by an Identification Service Agency. In essence, the secure data management system ensures that the ratification has been undertaken only by users whose identification by an Identification Service Agency and whose ratification subkeys remains valid and current.

Failure at any point in these checks results in the transaction being returned to the pre-ratification stage.

In a commercial transaction, the secure data management system undertakes a series of arithmetic checks. Firstly, it nets the transaction to ensure that both financial sides of the epitome balance. Failure at any point in these arithmetic checks results in the transaction being returned to the pre-ratification stage.

Secondly, if there are other transactions that are intended to be settled at the same time agreed for completion, the secure data management system nets all these transaction as a whole to ensure that they balance and there are no arithmetic errors.

Users in transactions have a choice upon which they have agreed before ratification. Where other transactions are dependent on a transaction and that transaction fails any of its checks, they may agree that all transactions are to fail as well. They may also agree that a series of transactions may settle up to the point that any one transaction fails. In the event that they fail to agree, they are deemed to have agreed that a series of transactions may settle up to the point that any one transaction fails.

Failure at any point in these arithmetic checks results in a transaction being returned to the pre-ratification stage.

Thirdly, from those transactions that successfully negotiated all checks, the secure data management system nets all payments to each financial institution so that it is capable of transmitting into the financial system a list of payments to be made and received by each financial institution as a result of settlement. This list includes name of parties, BSB number and account details.

Finally, the secure data management system nets all payments from all these transactions on the basis of a net

interbank position required if they are to settle across the Exchange Settlement Accounts operated by financial institutions with Central Banks. This results in a net payment position for all these transactions for each financial institution.

Once these netting steps are completed, the secure data management system transmits the lists of payments and the net interbank position to a Financial Settlement Manager.

The Financial Settlement Manager provides the connection into the banking system. It delivers the lists of payments and the net interbank position to the financial institutions and each Central Bank.

Upon completion of an interbank settlement for these transactions across the Exchange Settlement Accounts operated by financial institutions with Central Banks, the Financial Settlement Manager is notified. In turn, it notifies the secure data management system. Only upon being notified that interbank settlement has occurred and hence that there is an irrevocable commitment to pay funds for each transaction settled as part of the interbank settlement does the secure data management system release title to the goods and services that were purchased or transferred for the consideration of the financial payments.

When used for commercial transactions, the success of the secure data management system is dependent upon title to goods and services being inextricably tied to payments made for them. That is, that there is an automatic passing of title to goods and services occurring through the secure data management system upon the payment of consideration for them.

This cannot be done unless part of a commercial transaction conducted using the secure data management

system includes passing of a capacity to the transfer title to goods and services to the secure data management system.

Ways in which this can be done include novation, inclusion of title to goods and services into the secure data management system or the preparation of agreements to sell into the secure data management system. The last, of course, requires that any agreement to sell, when ratified and delivered, conveys title in goods and services.

Upon passing of title in goods and services by the secure data management system as intended by the ratification, settlement of a transaction is complete. The "snapshots" of the epitome that together make the complete agreement are encrypted by the one half of the encryption key pair in the hardware token issued to each user who created a "snapshot" and passed to the secure data management system. The secure data management system transmits the ratified "snapshots" to secure archival storage facilities chosen by the users. The secure data management system then notifies all users who are party to a successful transaction that their transaction has been completed.

The electronic instrument of this embodiment provides both a means of delivering title to goods and services to a secure data management system and a means of downloading details of payment made from a secure data management system to a person or persons entitled to payment in a way that enables them to negotiate, discount or assign the benefit of the right to an irrevocable payment received from a commercial transaction in the secure data management system.

The secure data management system in the form of an electronic conveyancing system is depicted in figure 1A.

An initial step in the use of the electronic conveyancing

system (not shown in figure 1A) for sale and purchase of residential land concerns identification. A party who is selling an interest in land must prove that he or she has the right to sell the land. To do this in the paper-based system requires that a vendor/registered proprietor produce a Certificate of Title standing in the proprietor's name. With the electronic conveyancing system of the present invention there is no proof of ownership or Certificate of Title; a vendor, for example, needs some suitable alternative means of demonstrating his or her right to sell the land. This is accomplished by the vendor's use of an identification and authentication device in the form of what is herein termed a "Land Card", a form of identification described in greater detail below, and matching the details of the vendor against the original records maintained by the relevant Land Registry. Furthermore, transactions in land require a written contract or its equivalent to be effective.

To demonstrate right and identity, and to provide a means by which binding contracts can be executed, the electronic conveyancing system requires that every party obtain a Land Card from an "Identification Service Agency". This Land Card uniquely identifies the person to which the Land Card is issued. Before a party can take part in a transaction, this Identification Service Agency requires each of the parties to a transaction to attend before the Agent and demonstrate their identity. If banks require that a customer present 100 points of identification to open a bank account (where, for example, a passport might be worth 50 points, an existing bank account another 30 points, a driver's licence 20 points, etc.), the Identification Service Agency might require 150 or more points including photographic identification and identification showing a date of birth.

Once satisfied with the identification of a party, the Identification Service Agency issues a Land Card that

enables that party to identify him- or herself electronically and uniquely via a computer connected to the Internet, and to digitally execute documents (in the form of electronic data) so as to create legally binding contracts.

As part of issuing a Land Card to a vendor, the Identification Service Agency requires the vendor to nominate a property that the vendor wished to use the Land Card in order to sell. No proof is required that the vendor is the proprietor of the land nominated; nor does the Identification Service Agency investigate whether or not a vendor is the registered proprietor of the nominated land. However, should a vendor nominate land that he or she has no right to sell, the vendor will find that no purchaser would buy that land from him or her and details of the land will first be compared with the records kept by the responsible Land Registry. Thus, identification of, say, John Jones of 13 Irving Street, Huntingdale, date of birth 23 Jan 1960 may be certain owing to John Jones' Land Card, but details of the land specified by John Jones would have to match the records kept by the Land Registry before a purchaser will agree to buy the land.

A vendor is also encouraged to obtain a title search from the Land Registry for the nominated land as part of the details provided in the Land Card issued to him or her.

A vendor's Land Card is issued for twelve months or until a transaction with the nominated land is lodged with Land Registry, whichever is the earlier. This limitation on a vendor's use of a Land Card is enforced by the "Transaction Authority" (discussed below) within the Land Card.

For purchasers, the Land Card is issued for a fixed (preferably one year) period and allows a purchaser to purchase as many properties in that time as he or she

wishes. A purchaser's Land Card does not authorize the purchaser to sell any of the acquired properties. Again, the Transaction Authority within the purchaser's Land Card ensures these limitations are enforced.

Other parties, such as real estate agents, legal representatives, conveyancers and bank officers, who undertake conveyancing as part of their professional duties, would hold a Land Card issued for a fixed one year period. They would then be able to act as the agents of others in any kind of conveyancing transaction but their Land Card would not permit them to buy or sell land on their own account. Again, the Transaction Authority within the Land Card ensures these limitations are enforced. It is envisaged that all those who deal professionally with land will obtain a Land Card as a means of doing business.

The identification provided by the Land Card and the matching of the land nominated and the vendor named in the Land Card with the land and its registered proprietor on the original records maintained by Land Registry replaces the Certificate of Title as demonstrating a vendor's entitlement to sell the land.

Upon the issue of each Land Card, an Identification Service Agency arranges for the creation of three key pairs, an identification keypair, a ratification keypair and an encryption keypair for the party to whom the Land Card is issued. One key from each keypair is uploaded to the Land Card and forms the basis for the identification, ratification and encryption functions required by the holder of each Land Card. All three functions are carried out asymmetric cryptography. The other half of each keypair is used by the Identification Service Agency and the secure data management system to verify the identification, the execution of all data and the data's encryption by the holder of the Land Card.

In a typical transaction, a vendor first obtains a Land Card and nominates the land he or she wishes to sell as the first step in selling a property. The vendor then logs on to a real estate agent's website and seeks to have his or her land listed for sale.

The first thing that the website of a real estate agent seeks from a vendor is proof of the vendor's identity, a proof provided by use of the Land Card issued to the vendor. The vendor then provides details of the property the vendor is seeking to sell.

Figure 1A represents the various steps in the electronic conveyancing process by reference to the information that is progressively added to the electronic "Coversheet" (described in detail below), an electronic representation of the information executed or otherwise) pertaining to the transaction.

Thus, from the details of the property the vendor is seeking to sell, a legal representative or conveyancer retained to act for the vendor is able to create the "Coversheet" 10 and obtain remotely a title search 12 and municipal and statutory information 14 with which to populate 16 the Coversheet 10.

By means of the Coversheet created by the first party to the transaction, the real estate agent and the vendor undertake negotiations about the commission payable and the terms of sale that the vendor requires by use of bid and counterbid. Once they agree, each uses his or her Land Card to execute a digital "Authority to Sell", the data of which (of the Real Estate Agent 18 and of the vendor 20) is incorporated 22 into the Coversheet at the "Authority to Sell" stage 24. This execution is undertaken using an " Ratification subkey" within the Land Card. Because an Authority to Sell is ordinarily a

standard form, only the data that is used to complete it is added to the Coversheet. All its standard terms and conditions are included by incorporation by entering the name of the published form and its publication details as part of the data or by incorporating a reference to a website containing the terms and conditions.
The step of retaining a real estate agent to act for a vendor is not essential in the electronic conveyancing system, but it is such a typical and common way of undertaking a sale of residential property that it is included in this description as part of the process of the electronic conveyancing system as an embodiment of the secure data management system

Once the digital Authority to Sell is executed, the real estate agent then begins the work of selling the property on behalf of the vendor.

Using the Coversheet to provide the details of the land that are required by every prospective purchaser, the electronic conveyancing system provides a method by which the listing and marketing of properties can be conducted via the Internet.

The next step in the conveyancing occurs when a purchaser expresses interest in the property. According to the electronic conveyancing system, an intending purchaser usually logs onto the real estate agent's website and uses a Land Card to identify himself or herself. The purchaser obtains a Land Card before beginning the process of purchasing, as a real estate agent will not enter into negotiations to sell with an unidentified person.

Once identified by means of a Land Card, the purchaser begins negotiations with the real estate agent using bid and counterbid. With the electronic conveyancing system of the present invention, these negotiations as to terms, conditions and price can occur via the Internet.

All the legal information about the property that might need to be provided and inspected by a purchaser is already available to the purchaser in the Coversheet.

Eventually, the purchaser makes an offer (executed using a Land Card) that the vendor can accept by using his or her Land Card to execute that acceptance. All purchaser information 26 provided by the purchaser (as to identity, value of offer, etc.) is inputted into the Coversheet at the "Contact of Sale" stage 28, as is contractual information 30 from the vendor.

The executed offer and acceptance constitute a legally binding contract, complete with all terms and conditions necessary for its enforcement. Base terms and conditions that can be specifically excluded by the parties will normally be provided by prevailing statutory provisions, combined with standard published terms and conditions incorporated, where desired, by reference. Any new data from the contract and any special terms that are not implied by Statute or incorporated from standard published terms and conditions are added to the Coversheet. This would include the name and other details of the purchaser, the price and the settlement date and time agreed. There is therefore no paper contract of sale. Instead, within the Coversheet is a collection of data that, together with the digital execution of the parties, makes up an enforceable contract.

Alternatives to Internet mediated contracts of sale in the electronic conveyancing system include sale at auction where the purchaser buys and signs off on - by means of a Land Card - the data in a Coversheet needed to create a legally binding contract. Another alternative is an electronic auction conducted via the Internet. The same underlying process used for the electronic conveyancing of land by means of the electronic conveyancing system can

also be used where the purchaser negotiates the contract of sale in the office of the real estate agent and then uses a Land Card to bring a legally binding contract into being.

Although the creation of the Coversheet occurs early in this exemplary transaction, the electronic conveyancing system merely requires that the parties create a Coversheet at some time before settlement. An entire conveyancing transaction (apart from settlement) could be conducted on paper and then, at some stage before settlement, one or more of the parties could create a Coversheet and enter the data described above so that the ultimate settlement is electronic.

After a vendor and purchaser have entered into a contract of sale, the vendor ordinarily notifies the vendor's mortgagee that a settlement of the sale and purchase is due at a specified time and date and requests 32 that the vendor's mortgagee should provide payout figures to the vendor.

With the electronic conveyancing system, the Coversheet contains the information that a vendor's mortgagee needs to provide payout figures. By notifying the vendor's mortgagee electronically and providing the mortgagee with access to the parts of the Coversheet containing the information required by the vendor's mortgagee, the vendor is able to use the data in the Coversheet to prevent the duplication of work. Details of funds needed to pay out the vendor's mortgagee are added 34 by the vendor's mortgagee to the Coversheet at the "Discharge of Mortgage" stage 36.

In paper-based conveyancing, the vendor's mortgagee ordinarily prepares a discharge of mortgage for exchange at settlement. With the present electronic conveyancing system, the vendor's mortgagee adds the new data needed to

create a discharge of mortgage to the Coversheet but does not execute the data.

In most cases of residential purchases, a purchaser needs to obtain mortgage finance in order to complete the purchase. With the electronic conveyancing system, this is undertaken by making a loan application (preferably a highly structured online loan application) to the financial institutions likely to lend and supplying them with access to those parts of the Coversheet provided by the purchaser that supply the information needed by a mortgagee to assess whether or not it should take a mortgage over the land.

By means of this online loan application and access to the Coversheet, a financial institution that might be interested in lending on the security of the purchase is provided with all the details about the purchaser and the property purchased that it needs to undertake assessment of the loan. Once the financial details provided by the purchaser are checked, the financial institution is then in a position to make a decision whether or not to grant a mortgage. There is no need to check the information that it obtains from the Coversheet. This has been provided and verified by Land Registry and the statutory and municipal authorities.

The Coversheet holds data in a common non-proprietary format, so the information contained in it can be readily downloaded and manipulated by those with access to it for their own back office processing.

If a financial institution agrees to lend money to the purchaser on the security of the purchase, it accesses the Coversheet, obtains any information it requires (including loan and mortgage information 38 from the purchaser) and adds 40 the new data 42 needed for a mortgage; the Coversheet is now at the "New Mortgage" stage 44. Statute

will imply the operative words required. While terms and conditions of the mortgage can be entered in the Coversheet, it will be convenient for most mortgagees to incorporate the wording of one of the Memoranda of Common Provisions held by Land Registry on their behalf.

Again, like all preceding parts of the transaction, this results in no paper documents and data entry is only required for new data items. The already existing data items are part of the Coversheet for the transaction and do not require re-keying.

The second last stage of a conveyancing transaction involves settlement. As pointed out above, in existing systems this involves the personal attendance of settlement clerks from all sides of the transaction to exchange money for the paper documents needed to obtain registration of the interests of the purchaser and purchaser's mortgagee.

According to the electronic conveyancing system of the present invention, settlement is undertaken remotely and need not be carried out by the parties at the same time. The details of the contract of sale initially agreed by the vendor and purchaser contains a time and date for settlement. At any time prior to that settlement time and date but after all data has been added, the parties each notify the secure data management system that they are ready to ratify the transaction. This notification serves as the means by which the secure data management system can retrieve the data needed for settlement. Referred to as an epitome, this data is transferred to the electronic conveyancing system's "Settlement Manager" (described below). Accessing the Settlement Software on their own computers, each reviews 46 the details of the transaction. Unlike paper based conveyancing, there is no execution of individual document. There are no individual documents; the users ratify the so much of the whole of the

transaction as it applies to each of them. Each must be satisfied with the terms and details of the transaction. Once satisfied, each ratifies 48 the transaction as a whole using his or her Land Card, thereby agreeing to all the components of the transaction in which that respective party played a part. This ratification results in the execution of the data held pertaining to the discharge of mortgage and the incoming mortgage, details of which were entered in the Coversheet but left unexecuted. It also overcomes any legal problems where early parts of the transaction might have been paper-based, which may be an issue during a transitional period after the introduction of the present electronic conveyancing system.

Even though all parties may have ratified the data contained in the Coversheet (now at Settlement stage 50), final settlement does not occur until the agreed time and date set for settlement. At any stage prior to that time, a party may abort settlement by withdrawing his or her ratification

This means that ratification is dependent upon two conditions being met:

1) all parties must review and then ratify all data; and

2) the time set for settlement must have arrived without a party withdrawing his or her ratification

Until both those conditions are met, any ratification is not binding on the party ratifying.

While in some jurisdictions a stamp duty (or equivalent tax) is self-assessed. If not, access to the unrestricted parts of the Coversheet is given to the State Revenue Office or other relevant authority before settlement. The State Revenue Office uses this data to pre-assess the stamp duty payable on the transactions and then commits the amount payable to the Coversheet. This amount must be paid as part of the financial transfers of funds

inherent in settlement.

Once the time and date for settlement arrives and all parties have ratified the data in the Coversheet in so far as it pertains to them, the settlement process is locked and irrevocable. The secure data management system in this electronic conveyancing embodiment takes the form of the aforementioned Settlement Manager ; the Settlement Manager checks and balances the transaction. More particularly, it conducts a check to ensure that the data is fit for lodgement (preferably in the form of a machine based check of the Registry's computer system).

If this process is completed satisfactorily, the Settlement Manager then nets all transactions occurring at that time. If this process is completed satisfactorily, the Settlement Manager prepares, for each financial institution involved in the transactions, a list of payments to be made and received with details of the parties' names and account details. Finally it prepares a net position for all financial institutions taking part. These last two items are passed to the interface to the banking system, called a "Financial Settlement Manager" which in turn passes them to the financial institutions and the Central Bank.

Payments of all money is made across the Exchange Settlement Accounts held with the Central Bank by the financial institutions, called in this embodiment "the interbank settlement". On completion of this interbank settlement, the Financial Settlement Manage notifies the Settlement Manager which then transmits 52 all data for lodgement with the local Land Registry 54 which formally lodges the data received by it as a discharge of mortgage, transfer and mortgage.

Upon completion of the lodgement of data with the local Land Registry, the financial data for the transaction is

committed through the Settlement Manager and transferred for uploading to the recipients' Land Card.

Should any part of this lodging or financial data fail before interbank settlement, or fail to return an acknowledgement before interbank settlement, all parts of the settlement fail and any ratification of the parties fails to become unconditional. To settle the transaction will require all the parties to set another time and review and ratify the transaction before that new time.

Should any part of this lodging or financial data fail after interbank settlement, or fail to return an acknowledgement after interbank settlement, payments of funds is irrevocable. Therefore, after interbank settlement all parts of the settlement must be reviewed, corrected and lodged. At the time of interbank settlement, all ratification of the parties becomes unconditional.

Once the acknowledgement of lodgement is received by the Settlement Manager, the information needed to update the records of municipal and statutory authorities 56 is transmitted to them using FTP 58.

Thus, advantageously in the electronic conveyancing system of this invention, the information remotely supplied at the start of the transaction by the Land Registry and by municipal and statutory authorities is used to provide the data elements that will be needed by the parties throughout the transaction.

Once placed in a Coversheet, this information is gradually enriched as the parties add their own new details at their own convenience. To obviate the task of re-entering data, the information contained in the Coversheet is made available to each of the parties to assist them in adding their own details.

When complete, this data and the original data is ratified by the parties and those parts of the information necessary to gain registration of the transaction are lodged remotely with Land Registry. After interbank settlement, all funds payable are irrevocably committed and acknowledgement of the commitment is electronically delivered to the parties entitled. These funds include those required for the payment of stamp duty and other government fees and charges. The municipal and statutory authorities are also notified of the change of details for their records.

Because some of the information provided by the parties is sensitive and confidential, the system provides parties with access only to the epitome of the transaction and any parts of the information controlled by them or to which they have been given access.
Information is added to the Coversheet from each step in the transaction and can be made available for use by one or more of the other parties. When complete, the data from the Coversheet required by them is lodged with municipal authorities.

As is shown in figure 1A, once each party has obtained a Land Card from an Identification Service Agency, they can - after first identifying themselves - execute parts of the transaction, including entering information and executing (viz. sign off on) various documents and therefore stages of the transaction, as well as ratifying those parts of the transaction that affect them at a time before the time and date agreed for completion. As a consequence, the vendor needs a Land Card to prove his or her ability to sell the land.

Figure 1B depicts schematically the electronic conveyancing system of figure 1A incorporating the secure data management system of this embodiment from the

perspective of the underlying system architecture and its interrelationships up to the time of settlement.

Figure 1C depicts schematically the electronic conveyancing system of figure 1A incorporating the secure data management system of this embodiment from the perspective of the underlying system architecture and its interrelationships during and after the time of settlement.

Referring to figures 2 to 4 (the legends for which are as shown in figure 2), the electronic conveyancing system includes a series of components known as "Land Trader", which provides the capacity for the electronic conveyancing system (or any similar secure data management system according to the present invention). Unlike other transaction engines or secure data management systems, Land Trader does not store the transaction data nor does it control the transaction process. Instead, it acts as the interface for the parties and to the mode of storage that a user wishes to use. It allows the retrieval of data from storage for formatting and presentation in the form of a Coversheet for viewing and modification by the parties. Control of the transaction process and storage of the data during the course of the transaction are solely within the control of the users.

Land Trader provides an end-to-end electronic transaction system - for conveyancing, in this embodiment - capable of operating over and by means of the Internet. Land Trader supports transactions involving a large number of parties to the transaction while minimizing the hardware and software requirements needed within Land Trader. It provides privacy for the personal information of each party; data content within and transferred by Land Trader is highly secure.

Figure 2 is a flow chart of the pre-settlement phase of

Land Trader's operation, while figure 3 is a flow chart of Land Trader's operation from settlement onwards. Figure 4 is a schematic representation of the hardware components of Land Trader. All traffic with Land Trader or generated by Land Trader is based on TCP/IP packets.

When a user, usually a vendor, logs on to Land Trader using his or her Land Card and seeks to create a Coversheet, the logon is to the system's User Interface Manager. This Manager is only a pass-through server that acts as the interface or traffic controller between the user's computer and other parts of Land Trader. It controls traffic by reference to its access and role controls. It does not store any data but operates to eliminate any direct access between the user's computer and other parts of Land Trader. The User Interface Manager does not control any part of the conveyancing transaction but merely directs traffic to the appropriate computer system according to the needs of the transaction and the wishes of the parties. At a party's logon, it will, for example, pass the logon to an Identification Service Agency to ensure that the user has a valid and current Land Card.

Referring to figure 2, when a user wishes to create a Coversheet, he or she inputs that request (and other data) 60 into the User Interface Manager 64 by means of his or her user computer 62 (after logging onto the User Interface Manager 64). The User Interface Manager 64 passes the request to a WebServer 66 supplying Single Data Entry Software. WebServer 66 responds by supplying that Single Data Entry Software to the user computer 62. Based on the jurisdiction chosen by the user, this software provides the forms and data entry templates to enable a user to fill in all the details necessary for a transaction in that jurisdiction.

It obtains these forms and data templates from a National

Conveyancing Data Dictionary 68. This is a dictionary that serves, to a user's computer, the forms and templates appropriate for the jurisdiction in which the transaction is to be registered.

Once the Single Data Entry Software has been downloaded onto the user computer 62, together with the forms and data templates appropriate for the jurisdiction of the transaction, the user is asked to specify the mode of storage in which the user wishes to store all data during the life of the transaction. This may be any central or distributed secure server to which the user has access on a subscription or other basis.

The user employs his or her own computer 62 to complete the information needed for the Coversheet. The user also remotely requests both a title search from the Land Registry computer system 70, and any required information from the appropriate municipal and statutory authorities 72, to be downloaded into the Single Data Entry Software. As each section is completed and committed by the user (still operating with his or her Land Card), that information is encrypted by the Land Card and uploaded to the User Interface Manager 64 by the user computer 62 for transmission through to the secure storage facility chosen by the user.

Where a user is a commercial user, he or she may choose to use proprietary software owned or licensed by him or her. In such a case, the presentation layer forming part, in this example, of Land Trader will act as the interface between the user's proprietary software and the User Interface Manager, enabling the user to use proprietary software.

Upon being provided with a fully qualified domain name or number for that mode of storage, the Single Data Entry Software or other proprietary interface to the

presentation layer sends a message to the storage system seeking permission to upload the encrypted data, and obtaining details of the required format. This message is passed through a Transaction Locator 74 and out through the User Side Storage Plugs 76 (see also figures 5 and 6) of Land Trader.

The Transaction Locator 74 stores pointers to the data stored in the mode of secure storage 78 chosen by a user. At the request of the user computer 62, the Transaction Locator 74 uses these pointers to request retrieval of the stored data for forwarding to the user. The Transaction Locator 74 only receives and transmit communications with the User Interface Manager 64 and the User Side Storage Plugs 76, and will accept messages from no computer system other than the User Interface Manager 64 and the User Side Storage Plugs 76, so it has a very high level of security. This first message it uses to create a set of empty pointers for a Coversheet. It then passes the message through the User Side Storage Plugs 76. The contents of the acknowledgement message is placed in one of the pointers and, like the rest of the pointers, can be used to rebuild all message traffic and its fate.

The User Side Storage Plugs 76 are essentially a four part interface to the method of storage chosen by the user. These Plugs 76 are used to direct the storage of data during the life of the transaction and consist of a data packet stream analyzer to direct and route traffic, a series of parsers to convert a data stream directed to them into a format capable of being handled by the receiving interface and a Random Balanced Packet Allocator.

The User Side Storage Plugs 76 first receive a request from the single data entry software or the user's proprietary software on the user computer 62 to store data from a transaction. This request is conveyed via the User

Interface Manager 64 and the Transaction Locator 74. Upon receiving directions as to the location of the storage and type of storage interface required, the User Side Storage Plug 76 will pass all incoming data packets through the analyzer to ensure that the packets are meant for parsing and not for message or acknowledgement. If data packets are to be parsed, the Plugs direct them to an appropriate parser that converts the contents of the data stream from its native encrypted XML format into a format applicable to the type of storage requested by the user. The output from the parser is then directed to the location of the storage 78 required by the user.

Acknowledgement of completed storage is then passed back through the Plugs 76 to the single data entry software on the user computer 62 via the User Interface Manager 64 and the Transaction Locator 74. The Transaction Locator 74 abstracts details of storage location and type from that acknowledgement and stores it as part of the pointers for the transaction of which the data package is a part. The remaining part of the acknowledgement is passed to the user computer 62 for storage in the single data entry software.

As there are other parties to transaction, they too download the Single Data Entry Software or use proprietary software and Land Trader's presentation layer, choose their mode of storage and enter data. At this stage, the data that they add to the Coversheet (see figure 7) and commit is transmitted to the User Side Storage Plugs 76 via the User Interface Manager 64 and the Transaction Locator 74.

To preserve the high levels of data integrity and security, the system optionally sends data to the User Side Storage Plugs encrypted as an entire package. That is, when data is sent for storage, the data sent will be sent entire. For example, if a name and address is sent

for storage, a user will have the option of sending both details encrypted as a single data package to the Plugs. Although this increases the difficulty of breaking the code used, it is not possible where the mode of storage chosen relies on tables based on fields that have a value for name and a value for address. It can also be defeated by a user who enters a name and commits it and then later enters an address and commits it. In other words, where a user commits data after the entry of every field, this higher level of security will not be achieved.

As most commercial databases are relational and hence will have field and table structure, the less secure option is necessary if a user wishes to send each item separately, that is, a name as a unique and separate data package and an address as another, separate data package.

To overcome this limitation without relying on storage methods that use large objects, the User Side Storage Plugs adopt another method, that of using a Random Balanced Packet Allocator. In this method, the data stream is allocated on a random basis, resulting in a balanced load of information being stored across the modes of storage chosen by all users; thus, the integrity of data and its security can be maintained even within the fields of a relational database.

Use of this Packet Allocator means that, although the mode of storage chosen by a party is used for storage of the transaction's details, the information stored in the mode of storage chosen by a user may not be the information entered by that user. That is, the User Side Storage Plugs use packet allocation to allocate storage evenly between the modes of storage chosen by the parties to a transaction. The allocation of the data packet to be stored in any particular mode of storage is determined at random but the total amount of storage used is proportionately shared across the modes of storage used by

all parties to the transaction. As each party joins the transaction, the mode of storage chosen by that party forms a pool to which information is allocated. Committal and retrieval results in the gradual reallocation of the data packets to ensure that there is a proportionate sharing of each mode of storage for the data. The random nature of the use of each mode for any particular data packet means that User Side Storage Plugs allow the use of inherently unsafe storage accommodation if this is desired by users. Although elements of a transaction may be lost, the loss of all elements of the transaction is remote as is the possibility of alteration of packets and hence of the transaction. This is achieved by the User Side Storage Plugs through their use of encrypted packets and the balanced allocation of random data packets to the modes of storage chosen by each party to the transaction.

Even in the event of deliberate attack, the field allocation in a relational database does not weaken the encryption used. The information provided to an interface conforms to the field structure of that database but data contained in the field may not be the data named. The Transaction Locator, not the relational or other database in which the data is stored, is responsible for maintaining the details of the location of any given data packet.

The data can only be retrieved by using the Transaction Locator. Any other attempt will result in the retrieval of meaningless data packets that may pertain to any part of the transaction, not merely the data items provided by the user who chose the mode of storage.

Pointers to each packet are maintained in the Transaction Locator.

The virtue of the User Side Storage Plugs is that they store no data and allow parts of a single data stream to

be transmitted to very different destinations that have totally different interfaces. By employing packets, these Plugs can act as a single balancing random switching and routing device into which one data stream is sent and three or more data streams emerge, each transformed into a form that can be transmitted to the appropriate interface.

Further, because the User Side Storage Plugs rely on packet switching and routing and a set of software filters or parsers for their working operation, their output can readily be modified to suit local needs simply by the addition or replacement of software filters.

The use of User Side Storage Plugs means that the storage requirements arising during a transaction are simplified. These requirements thereby become portable and generic. In the case of the electronic conveyancing system, the portable and generic nature of these Plugs is used to provide differentiated storage accommodation that can be chosen by a party or parties to the transaction.

Retrieval of data for a party operates similarly. A request for data is made from the Single Data Entry Software on the user computer 62 and referred via the User Interface Manager 64 and the Transaction Locator 66. The Transaction Locator 66 adds to the message passed to the User Side Storage Plugs 76 the details of the storage location and type. This storage location is used by the User Side Storage Plugs 76 to recover the data from the secure data storage 78 chosen by the user. The storage type location is used by the User Side Storage Plugs 76 to pull the recovered data through the appropriate parser that converts it from the form required for data storage back to encrypted XML format. Once parsed, the data is then returned to the user computer 62 via the Transaction Locator 74 and the User Interface Manager 64.

There are several points to note about User Side Storage Plugs 76. Firstly, even though the format of the incoming data package changes from XML to the appropriate format needed for storage, the data package remains encrypted. Secondly, the Transaction Locator 74 maintains pointer records for all data, even if not part of the final transaction so it is possible to ascertain the form of the transaction and the parties' agreement to the transaction at any time during the life of the transaction.

This approach to the storage of data supporting transactions has a limitation. In the event that the mode of storage chosen by the user is offline or otherwise unavailable when a user seeks to retrieve a data package, the User Side Storage Plugs 76 return an error message but not the requested data. Similarly, in the event that the mode of storage chosen by the user is offline or unavailable when a user seeks the storage of data, the User Side Storage Plugs 76 return an error message, but cannot store the data. The user, in this latter case, must send the data package for storage later when the mode of storage chosen by the user is online.

As the transaction moves towards completion, more and more data is stored in the modes of storage chosen by the parties.

Referring to figure 3, when a party is ready to begin the settlement process, he or she informs the Single Data Entry Software or his or her proprietary software that interfaces with the Land Trader's presentation layer. At this stage, the Single Data Entry Software or the proprietary software notifies the User Interface Manager 64 that settlement is imminent and through the User Interface Manager provides the Transaction Locator with sufficient detail to recover the data needed from the transaction's epitome from the secure storage used by the parties.

The Transaction Locator transfers the retrieved epitome to the Settlement Manager and the User Interface Manage transfers the user to the Settlement Software (on user computer 62) while, in turn, the User Interface Manager 64 directs its connection from that party to the Settlement Manager 80.

From this stage onwards for that party, the party who is ready to settle deals with the Settlement Manager 80, albeit through the User Interface Manager 64.

The first step in the settlement after logon is a review of the transaction. The Settlement Software formats the epitome of the data from the transaction it has received from the various modes of storage adopted by the respective parties and displays those parts of it to which each party has access according to the epitome template it has received from the User Interface Manager. When each party is satisfied that all parts are complete and in accordance with the transaction which he or she intended to enter, each respective party uses his or her Land Card to ratify the transaction in so far as it pertains to that party.

As there is little point to reviewing a transaction unless it is complete, the other parties will follow suit by transferring to Settlement Software and the Settlement Manager 80 shortly afterward.

However, a strength of the Settlement Manager 80 is that it permits asynchronous settlement. Each party reviews the transaction and ratifies it at his or her own convenience. As each ratification occurs, the Settlement Manager 80 meets another condition needed for final settlement. The Settlement Manager then acts as a gateway that only opens when all parties have ratified and the time and date for settlement are reached.

Finally, when all parties have ratified and the time for settlement is reached, the Settlement Manager 80 opens the gateway and begins the checking and balancing process described above. When it has completed all four netting processes it transmits all relevant financial details to the Financial Settlement Manager that transmits them in turn to the financial institutions and Central Bank for interbank settlement across the institutions' Exchange Settlement Account. When interbank settlement is completed, the Financial Settlement Manager transmits acknowledgment of the interbank settlement to the Settlement Manager. The Settlement Manager, in turn, transmits the details of the epitome of the transaction and all ratifications of the epitome to the Land Registry 82. The Settlement Manager 80 stores nothing but the settlement state, that is, the set and state of ratifications and the time of settlement, so the Settlement Manager 80 calls the data from the mode of storage chosen by the parties. The data is retrieved in the normal way via the User Side Storage Plugs 76 except that the information is not displayed on the user computer 62. Instead, details of the epitome for the transaction and all ratifications are transmitted to the Land Registry 82.

The parties, if they wish, may undertake a remote check title search at any time up to the time for settlement from the Settlement Software on their computer 62. This ensures that they are not committing to a transaction that has been previously lodged that would be defeated or postponed by a lodgement already in Land Registry 82.

At any time before settlement, the parties can undertake a remote identification check with an Identification Service Agency 84 from the Settlement Software on their computer 62. This allows them to satisfy themselves that the other

parties identified as being part of the transaction are those with whom they believe they are doing business.

Once the time for settlement has been reached, the Settlement Manager 80 proceeds to settlement. While settlement is underway, the Settlement Manager 80 will accept no further data from the parties. If not all parties have ratified at the predetermined settlement time and date, the settlement will immediately abort and all parties will have to re-ratify the epitome of the transaction and enter the Settlement Software and Settlement Manager 80 again.

Successful settlement is also dependent upon Land Trader and all required computer systems remaining online at all times during the settlement process up until the moment of interbank settlement. The required computer systems are those of the paying and receiving parties and the mode of storage chosen by the parties. Any failure of online status immediately aborts the settlement. All parties will then have to re-ratify the epitome of the transaction and enter the Settlement Software and Settlement Manager 80 again.

If Land Trader and all required computer systems do not remain online at all times after the moment of interbank settlement, the settlement continues, but is completed only once Land Trader and all required computer systems come back online.

Once notified by the Financial Settlement Manager that interbank settlement has occurred, the Settlement Manager arranges for the epitome of the transaction and all parties' ratification to be transmitted to the Land Registry 82 via the Transaction Storage Plugs 86. The Transaction Storage Plugs 86 discard any parts of the epitome not needed for lodgement with the local Land Registry.

The computer system of the Land Registry 82 then uses a combination of business rules and reasonable probability to ascertain the likelihood of successful registration. Where data is otherwise unverifiable, it accepts it, provided it has been executed by the parties concerned and then ratified by all parties at settlement. An example of this is consideration. Although the amount of consideration can be partially verified by business rules and reasonable probability, it is intrinsically incapable of validation. However, if the State Revenue Office, the vendor and purchaser and the purchaser's mortgagee have accepted the details concerning consideration, it is reasonable to accept them. In this case, the amount would also be reflected in the lodging fee payable to the Land Registry and must be the basis on which the lodging fee is calculated.

All such data items from the epitome in which the local Land Registry 82 is interested for lodgement are capable of multiple level verification. If this verification succeeds, the local Land Registry 82 will advise the parties of a successful registration. Where there are problems in passing the epitome for registration, the local Land Registry will contact the party responsible and arrange for correction or withdrawal.

At lodgement, however, the transaction is complete. At that stage, the Settlement Manager 80 passes the message received from Financial Settlement Manager 88 which is the interface to the financial system and the paying financial institutions . The funds transfer messages are passed from the receiving financial institutions to the Financial Settlement Manager 88 after interbank settlement that the funds are to be transferred to the accounts of the receiving parties. The funds transfer messages are passed to the receiving parties' computers so that they can

receive a copy of an "Electronic Bank Receipt" (described below). On receipt, the data from the Coversheet is formatted into the Electronic Bank Receipt and uploaded to the Land Card of receiving parties through a "Parasitic Operating System" (also described below) on their computers.

If the Land Card of any receiving party fails to acknowledge receipt of the correct amount (through an "Authorization and Display Processor") on the Land Card, the Settlement Manager immediately notifies the financial institution concerned that download of the Electronic Bank Receipt was not completed. This will result in the financial institution refusing to honour the Receipt.

After lodgement, dealing numbers are transmitted to the Settlement Manager 80 by Land Registry. The Settlement Manager in turns passes these through the User Interface Manager 64 to the Settlement Software on the users' computers for acknowledgment.

Upon receiving acknowledgement of dealing numbers from the computer system of the Land Registry 82, the Settlement Manager 80 undertakes a file transfer protocol (FTP) download of the information in those unrestricted parts of the Coversheet that is normally delivered to all relevant municipal and statutory authorities 90 after settlement.

Upon receiving acknowledgement of dealing numbers from the computer system of the Land Registry 82, the user is then in a position to download from secure storage the parts of the Coversheet that he or she controls or to which he or she has access to the modes of secure storage 92 chosen by that user for indefinite long term archival storage. If a user requires, he or she may print the parts of the Coversheet that he or she controls or to which he or she has access.

All data streams and acknowledgements within the settlement process take only several seconds and appear to be effectively simultaneous to the user. After they are complete, the parties are automatically returned to their Single Data Entry Software for any further transactions.

ADDITIONAL DETAIL CONCERNING VARIOUS COMPONENTS OF THE ELECTRONIC CONVEYANCING SYSTEM

A. Land Trader (see figures 2, 3 and 4)

Land Trader, a generic transaction engine, has a number of components:

1. User Interface Manager - This Manager is only a pass-through server that acts as the interface or traffic controller between the Transaction Locator, the user's computer and the computer system of the Identification Service Agency. It does not store any data. It ensures that the User's computer does not need direct access to the Transaction Locator or the computer system of the Identification Service Agency ensuring higher level of security for these systems. The User Interface Manager does not control the transaction but merely directs traffic to the appropriate computer system according to the needs of the transaction and the wishes of the parties. It also passes the logon of a user to an Identification Service Agency for the purposes of determining whether the identification key used by that user is valid and remains current.

2. Transaction Locator - This component stores pointers to the data stored in the mode of storage chosen by a user. When requested by a user's computer, the Transaction Locator is able to use these pointers to request retrieval of the stored data for submission to the user. Because the Transaction Locator only receives and transmit communications with the User Interface Manager and the User Side Storage Plugs, its level of security can

be made extremely high. It will accept messages from no computer system other than User Interface Manager and the User Side Storage Plugs.

3. User Side Storage Plugs (see figure 5) - These are the interface plugs that enable the mode of storage during the life of the transaction to be chosen by a user and "plugged" into Land Trader. These free Land Trader from any need to store data from transactions. It also enables users to choose the level of safety and security they choose for the storage of their data.

Within the User Side Storage Plugs are three subcomponents:

a. Data Packet Stream Analyzers - One for internal incoming data and the other for external incoming data, these analyze a stream of data packets and route them to their destination within the User Side Storage Plugs according to their headers and the business rules established for data packets with particular headers.

b. Parsers - These convert the contents of the data stream directed to them from the data stream's encrypted XML format into a format and interface structure applicable to the type of storage requested by the user.

c. Random Balanced Packet Allocator - This is a software application that is available if requested by user. It allocates data packets for storage on the basis of balancing storage use evenly between the modes of storage chosen by the parties to a transaction. Within each proportionate allocation of data packets to storage use, the allocation of the data packet itself is random.

As a party joins the pool of parties offering storage, the Random Balanced Packet Allocator re-allocates the proportionate balance of storage space used to include the new party's storage. Committal and retrieval of stored data are the means by which the Allocator gradual reallocates data packets to ensure that there is a proportionate sharing of each mode of storage for the data.

The random allocation of particular data packets to any given storage point within the total storage pool ensures that high level encryption is maintained without there being any correlation between the contents of the data packet and the party who committed them to storage.

The data packets committed to a storage point within the total storage pool conform to the field structure and data format of the database used for storage but the data stored in the field may not be the data named. The Transaction Locator, not the relational or other database in which the data is stored, is responsible for maintaining the details of the location of any given data packet.

The data can only be retrieved by using the Transaction Locator. Any other attempt will result in the retrieval of meaningless data packets that may pertain to any part of the transaction.

4. Settlement Manager (see figures 13A, 13B, 13C and 13D) - When a transaction is ready to settle, the User Interface Manager directs all traffic from a user's computer to the Settlement Manager. This is a server with the task of retrieving an epitome of the transaction to match the form of the template provided for that transaction and then conducting a series of checks to

determine the suitability of a transaction to settle. If this is satisfactorily completed, the Settlement Manager then undertakes a four level netting process of the transaction that are to be settled at that time. Once completed, lists of payments and receipts and net bank position are forwarded to the Financial Settlement Manager. It does not control the settlement process, nor does it store data. It does not authorize or control the settlement process but acts only to prevent settlement until all parties have confirmed the transaction and the time established by the parties has arrived. Although it conducts a series of checks of every transaction, it does not validate the settlement so that it can progress. This is the role of the parties. The Settlement Manager acts as a time based gateway. When all parties have ratified the transaction, the Settlement Manager calls the data needed for settlement from the User Side Storage Plugs and transmits it to the parties requiring to completed settlement. It is also the Settlement Manager that directs and transmits the acknowledgements from settlement and aborts settlement if appropriate acknowledgements and data are not transmitted and received.

5. The Financial Settlement Manager (see figure 1C) - This is an entry point into the banking system. It does not store data. Its sole tasks are to send financial information from the transaction to the financial institutions and to the Central Bank before interbank settlement, receive and forward notification of interbank settlement to the Settlement Manager and financial information necessary for the creation of an electronic bank receipt from the financial institutions after interbank settlement.

6. The Presentation and Transport Layers and their toolboxes (see figures 1B and 19) - The presentation layer is a means by which data being transmitted to a

user's proprietary software can be restructured and reformatted to make the data capable of being integrated with the user's proprietary software. The layer is based on a series of classes and an XML schema derived from these classes. The transport layer is a means by which data being transmitted to a proprietary software used for secure storage or by the financial institutions can be restructured and reformatted to make the data capable of being integrated with that proprietary software. The layer is based on a series of classes and an XML schema derived from these classes. The toolboxes for each layer are a "drag and drop" set of tools that enable a computer literate person to restructure and reformat data in a way that integrates it into a proprietary format without need to undertake programming to achieve this.

67. Transaction Storage Plugs (see figure 6, the legend for which is as shown in figure 5) - These are the interface Plugs that enable proprietary format storage to be "plugged" into Land Trader in order to take finalized data from a transaction for long term storage. For example, some information from a transaction needs to be stored in the Land Registry, other data is required for bank records and others is needed for municipal and government records. These operate databases in proprietary formats. The Transaction Storage Plugs provide an interface that translates data transmitted through the Settlement Manager into a format that is readable by these proprietary formats. Use of these Plugs free Land Trader from any need to provide long term storage of data from transactions. They also free Land Trader from the need to interface directly with proprietary databases.

These Plugs are essentially a two part interface for the lodgement and storage of parts of the Coversheet on

completion of the transaction. Made up of Data Packet Stream Analyser and parsers, these Plugs are used to transfer the parts of the Coversheet at the conclusion of a transaction to:

- the Land Registry for lodgement and registration of the data so that title is passed to the incoming purchaser;
- a State Revenue Office and municipal and statutory authorities for updating of their records; and
- The storage modes chosen by the parties for indefinite long term storage.

Each component performs the following tasks:

- Data Packet Stream Analyzers - One for internal incoming data and the other for external incoming data, these analyze a stream of data packets and routes them to their destination within the Transaction Storage Plugs according to their headers and the business rules established for data packets with particular headers; and
- Parsers - These convert the contents of the data stream directed to them from the data stream's encrypted XML format into a format and interface structure applicable to the type of storage requested by the user and vice versa.

These Plugs are also the interface that forwards messages concerning the payment of funds to the respective parties, including uploading of these details where necessary to the Land Card of those entitled to enable negotiation of financial components of the transaction.

These Plugs store no data and allow parts of a single data stream to be transmitted to very different destinations that have totally different interfaces. By using packets, these Transaction Storage Plugs can act as a single automatic switching and routing device into which one data stream is sent and three or more data streams emerge, each

transformed into a form that can be transmitted to the appropriate interface.

Because the Transaction Storage Plugs rely on packet switching and a set of software filters or parsers for its working operation, its output can readily be modified to suit local needs simply by the addition or replacement of software filters.

Transaction Storage Plugs mean that the storage or update requirements arising from a transaction are made simple. These requirements become portable and generic.

In the electronic conveyancing system, the portable and generic nature of these Plugs is used to provide differentiated storage accommodation that can be chosen by a party or parties to the transaction.

Unlike User Side Storage Plugs, Transaction Storage Plugs do not rely on random packet switching between storage modes to maintain data integrity. The data streams are differently structured and have different locations.

For example, it can be presumed that financial institutions and those bodies responsible for updating records of transactions will maintain high levels of data integrity and security. Therefore, the transmission of a data stream to them in a form encrypted at the interface of the Transaction Storage Plugs and then decrypted by them in their own computer systems will maintain these levels of integrity and security, provided it is supplemented by full message acknowledgement.

For modes of storage chosen by users for indefinite long term storage of transactions, there can be no such presumption. However, it must be for these users to ensure the safety of their storage choice.

The Transaction Storage Plugs maintain security and integrity by the use of encrypted data transmission to all storage. Because the data stream is relatively substantial, encryption by the Transaction Storage Plugs and the stream's decryption by the interface of storage systems maintain transmission security without the need for random switching of data packets.

Parties receiving messages concerning the payment of funds include:

- Land Registry regarding lodgement fees;
- State Revenue Office regarding stamp duty;
- Any financial institutions regarding the funds needed for the repayment of any outstanding mortgages; and
- Other parties, including the vendor, entitled to funds as a result of the transaction.

The Transaction Storage Plugs begin operation at the time of settlement. For ease of description, their operation is best described in several parts:

a. Retrieving Stored Data for Settlement

At settlement, a user requires access to the data stored through the User Side Storage Plugs. The request for this data is conveyed from the Settlement Software on the user's computer to the User Side Storage Plugs and is transmitted via the Settlement Manager, the User Interface Manager and the Transaction Locator.

As the request is passed through the Transaction Locator, it picks up the location and type of storage interface of the data and passes these through the User Side Storage Plugs. The User Side Storage Plugs then retrieves the data using the location indicators provided by the Transaction Locator. Using the

details of the storage interface provided by the Transaction Locator, the User Side Storage Plugs passes the incoming data package through the appropriate parser.

The data package, now converted back to its native encrypted XML format, is passed by the User Side Storage Plugs to the Settlement Software on the user's computer. The data package is transmitted via the Settlement Manager, the User Interface Manager and the Transaction Locator.

Acknowledgement of completed retrieval is then passed back to the Plugs from the Settlement Software on the user's computer via the Settlement Manager, the User Interface Manager and the Transaction Locator.

The Settlement Manager notes the transmission of the data package and its acknowledgement. Should there be any failure of receipt or acknowledgement, the rest of the settlement will abort and roll back to its starting position.

The user is now in a position to begin settlement by reviewing the transaction and ratifying it.

b. Dealing with Funds (see figures 15A, 15B and 15C)

Upon receiving acknowledgement from the Financial Settlement Manager that interbank settlement has occurred, the Financial Settlement Manager passes details of the irrevocable payments made to the Settlement Where a user is entitled to funds, the Settlement Manager uploads details of the funds entitlement to the Land Card of the user entitled as an Electronic Bank Receipt.

Acknowledgement of the display and uploads is then

passed back to the Settlement Manager from the user's computer.

The Settlement Manager notes the transmission of the financial data package and its acknowledgement and returns the acknowledgement to the Financial Settlement Manager for transmission to the financial institution of the user entitled.

Prior to settlement, the details of the Electronic Bank Receipt that will be received upon the completion are ratified by the parties as part of the epitome.

Once settlement occurs, the upload of the financial details into the Land Card of the user entitled results in the creation of an Electronic Bank Receipt that is negotiable by a receiving party to the extent that it establishes funds payable to that receiving party. However, it would be uncommon for a receiving government body or financial institution to seek the uploading of an Electronic Bank Receipt to its Land Card. Where funds are payable to these organizations, the usual overnight banking processes of financial institutions would ordinarily be used to arrange payment to them by having a receiving bank credited with the account due.

Although this settlement process has been explained with reference to settlement across the Exchange Settlement Accounts held by financial institutions with a Central Bank and less critical payments being made to a receiving bank crediting accounts for later payment, this approach can equally be used where settlement is arranged through payments that are paid and received by a clearing house.

c. Dealing with Records Updates (see figures 15A, 15B and 15C)

Once settlement begins, users use the software on their own desktop computers to review and ratify the distributed data retrieved from secure storage via the User Side Storage Plugs. The Settlement Manager stands between the parties and transmits the distributed data that is available to all parties so that each of them can review and ratify the transaction insofar as it applies to them.

The information controlled by a user or to which a user has access can be retrieved at any time from the mode of secure storage chosen by the user via the User Side Storage Plugs.

At Settlement, all data from the transaction is transmitted for indefinite long term archival storage as set out below. During settlement, all data required for update of municipal and statutory authority is transmitted as part of the lodgement process after interbank settlement.

8. WebServer supplying Single Data Entry Software - This supplies Single Data Entry Software to a user's computer. This software provides the forms and date entry templates to enable a user to fill in all the details necessary for the transaction. A user uses his or her own computer to complete this information. As each section is completed, it is uploaded to the User Interface Manager by the user's computer for transmission through to the mode of secure storage chosen by the user.

9. National Conveyancing Data Dictionary - This is a dictionary that serves to a user's computer the forms and templates appropriate for the jurisdiction in which the transaction is to be registered.

The software for Land Trader comprises:

a. Single Data Entry Software incorporating secure messaging, access, community, negotiation and execution software;

b. National Conveyancing Data Dictionary;

c. Jurisdiction specific stylesheets and templates for Single Data Entry Software;

d. User Side Storage Plugs, parsers and storage interfaces;

e. Encryption and Decryption tools for transmission and storage of XML based data;

f. Presentation and Transports Layers and their toolboxes;

g. Settlement Manager;

h. Financial Settlement Manager;

i. Land Card verification, identification, execution and download capacity for Electronic Bank Receipts (provided in conjunction with Identification Service Agencies);

j. Logon validation and verification software to ensure that the identification of a user remains valid and current;

k. Checking software that checks for "sanity", completeness and accuracy, and undertakes arithmetic tests of all ratified transactions;

l. Netting software that nets a transaction, nets a series of transactions, prepares a list of payments for transactions settling at the same completion time and nets the overall position of the financial institutions involved in the transactions;

m. Electronic Fund Transfer software, including uploading of Electronic Bank Receipt onto Land Cards (provided in conjunction with financial institutions);

n. Index software for Transaction Locator to provide pointers to data;

o. Secure identification and message transmission software for User Interface Manager; and

p. Transaction Storage Plugs, parsers and storage

interfaces (provided in conjunction with financial institutions, municipal and statutory authorities and Land Registry).

B. The Coversheet (see figure 7)

The Coversheet is central to Land Trader and transactions carried out using it, and may - as a data abstraction - be considered to be a file to which all parties contribute and parts of which are transferred to Land Registry at the conclusion of the transaction.

However, only as a data abstraction could it be considered as a file. Rather, it comprises six components held in different locations that, when retrieved and reassembled at the instruction of a user conveyed by the software on his or her computer, provide the Coversheet in a format that appears to a user to have the properties of a file. Because some of these components provide security or restrict access, they themselves may be not visible to a user of a Coversheet. However, a user will see the components' results or effects.

The components of the Coversheet are:

1. Data - This is the information initially provided by the Land Registry and the municipal and statutory authorities concerning the property being sold and purchased. Throughout the transaction, it is augmented by the parties to the transaction. At the completion of the transaction, the data is confirmed by the parties as being correct and is then transmitted to the Land Registry for registration of the interests being transferred. The municipal and statutory authorities are also notified so that they can update their records. Data from the Coversheet is held in the method of secure storage provided by or specified by the users.

Although the Coversheet comprises a number of components, it is a single entity. It is not made up of multiple copies of the same data that are merged upon retrieval. All data items are only stored once. Each data item may be stored in a different place but when placed together, these items constitute only one data set. For example, a vendor's name and other details may be stored in the secure storage chosen by the vendor. The purchaser's name and personal details may be stored on a central secure server to which the purchaser has a subscription. Details of the loan arrangements may be stored on a distributed secure server operated by a financial institution. However, when a party to the transaction seeks the retrieval of data, these data elements would be retrieved and presented to a user as one set of integrated data.

2. Pointers - This component of the Coversheet ensures that the data elements can be retrieved and presented as one set of integrated data. Instead of storing data within Land Trader, these pointers are stored in the Transaction Locator. The pointers point to the location of the data, whatever the data's storage mode or modes. The method of storage location and retrieval adopted for the Coversheet means that Land Trader cannot guarantee that the data is available at any given time. Land Trader, through the use of its component Transaction Locator, is able to locate where the data is being stored. The availability of data depends on the parties to the transaction and the arrangements that they have made with a provider of secure storage. This gives the parties control over the transaction and faithfully reflects the current paper-based conveyancing system.

3. Identification and Execution - The Coversheet provides reliable identification, important in any

system of electronic commerce. For the purposes of conveyancing, an agreement in writing is needed to pass any interest in land. Therefore, for conveyancing, Land Trader provides a means of ensuring there is an enforceable agreement, while the Land Card provides high level identification and allows the parties to execute a contract electronically. (See Section C below for further details concerning the Land Card.)

The Land Card is provided as a portable hardware device or token issued to an applicant at the same time that the applicant demonstrates his or her identity, and enables a party to a transaction to prove his or her identity to others in the transaction. The Land Card also enables a party to indicate the execution of the contractual information contained as part of the data of the Coversheet. The Land Card also enables a party to indicate his or her ratification of the complete transaction contained for which the Coversheet was created.

A transaction under Electronic Conveyancing is made up of a number of subtransactions, so identification and execution will occur for each of the subtransactions. At settlement, each party uses his or her Land Card to gain access to those parts of the Cover sheet which that user controls or to which that user has access. The identification key issued to the user and stored in the Land Card makes this possible. At that point, each party also uses his or her Land Card to execute a ratification of the transaction before the settlement can proceed. The ratification subkey issued to the user and stored in the Land Card makes this possible. Details of each identification and execution are encrypted by the Land Card itself and then transmitted in an encrypted form with the data elements to which the

identification and execution pertains to the method of storage chosen by the user. The encryption subkey issued to the user and stored in the Land Card makes this encryption possible.

4. Differential Access Rights - Some of the information provided by parties to a transaction is sensitive, so Land Trader provides a structure as part of the Coversheet that ensures that only the party controlling information or a party authorised by that party to have access can access any information. While the present system preferably incorporates security processes common to other secure systems as required (for encryption, login security, etc.), the Coversheet also limits access by requiring a party to specify the role in which he or she will be acting in the transaction. For example, the role chosen may be that of a purchaser, vendor, vendor's mortgagee and so on. Except for a vendor (discussed below), a party may initially choose to act as any party (see figure 9A: "choose class of party to transaction"). However, once a party chooses the role in which he or she will act, business rules applicable to that role determine the rights of the user in accessing data in the Coversheet and the tasks that that user may undertake in the Single Data Entry Software. The User Interface Manager will also prevent any attempt to access data in a way that is inconsistent with the role chosen by the user. Access to data not normally available to a user in a specific role may be provided by authorization. Authorization to data normally restricted by a particular role can be provided to any party by a person acting in that role.

5. Transaction Authority - Any party may seek and obtain more than one Land Card. However, to prevent a vendor from selling the same parcel more than once,

the Land Card of a vendor is linked to a parcel of land (referred to as the "Vendor's Link"). The parcel of land is nominated by the vendor at the time the Land Card is issued to the vendor. An Identification Service Agency makes no comment about whether or not a vendor is the registered proprietor of the land.

It remains the responsibility of a purchaser to determine the question of proprietorship. The Vendor's Link forces a vendor to specify the land for which the Land Card is issued. Should a vendor apply for another Land Card, he or she may specify the same or other land as the Vendor's Link.

The Vendor's Link means that the Land Registry will accept only a dealing with the land specified in a Vendor's Link by a vendor where the Land Card used is the first Land Card used by that vendor to ratify a dealing with that land. Any later dealing with the land by the vendor will be refused by Land Registry. Although a vendor may have another Land Card in which the Vendor's Link pertains to same land, the Land Registry will only accept the first lodgement of a transaction with the land by the vendor.

This right to sell land by a vendor, known as a Vendor's Transaction Authority, is part of the Differential Access Rights.

Once a transaction has been completed by a vendor using a Land Card with a Vendor's Link for that land, the Identification Service Agency will be notified by the Settlement Manager as part of the settlement process. On any later inquiry, the Identification Service Agency will notify a party inquiring that the Transaction Authority issued with the vendor's Land Card has now been cancelled.

For such a vendor, the identification system within the Land Card is still operative and can be used for identification of the vendor. However, upon lodgement of the transaction, the vendor's Transaction Authority expires and cannot be used by the vendor to carry out a transaction with the same land.

As part of the Differential Access Rights, the Vendor's Transaction Authority is unique. It prevents a vendor selling the same asset twice. It allows multiple issue of Land Cards to the same person, simplifying the management and record keeping for Land Card issue, but at the same time, prevents a vendor/registered proprietor from using a Land Card as a security for financial accommodation.

Like all other Differential Access Rights, the Vendor's Transaction Authority is maintained as part of the rule set maintained by the User Interface Manager. As with the Vendor's Link, a copy of the Transaction Authority is maintained within the Land Card.

C. The Land Card (see figures 8 to 12)

The Land Card is a portable hardware device or token issued to a person who attends in person before an Identification Service Agency and demonstrates to the satisfaction of the Agency that he or she is the person claimed. As discussed above, if a bank is required to obtain 100 points of identification before opening a bank account for a customer, an Identification Service Agency would require 150 or more points of identification. Identification must be in person and must be accompanied by at least one item of identification that demonstrates a date of birth. To ensure the continuity of identity with

the identification, the Land Card must be issued by an Identification Service Agency at the time that an applicant attends the Agency.

To maintain the integrity of the security and the identification processes that underlies the Land Card, all Land Cards have a limited life span of one year from the time of issue. As previously pointed out, the Land Card for a vendor has another inherent time limit. Once used to ratify and lodge a transaction, the Land Card for the vendor ceases to authorize a vendor to deal with the land nominated as the Vendor's Link in the Land Card irrespective of the life that the Land Card may otherwise have.

There are three classes of Land Card. The Vendor's Land Card has been discussed above. The second class of Land Cards, the General Land Card, also has a one year life but would be used by any person who does not act as the agent of another in conveyancing. It may be used at any time for any number of dealings, except disposition of an interest in the fee simple. For any transaction that involves a party disposing of an interest in the fee simple which, under paper-based conveyancing, would require the production of a Certificate of Title to the Registrar of Titles to gain registration, a party will need a Vendor's Land Card.

The third class of Land Card has the same life but is used when a person acts as the agent or employee of another. Unlike other Land Card types, this Land Card allows a party to act in an unlimited number of transactions during its life and permits the party holding it to act for another in disposing of an interest in the fee simple. Its limitation is that the holder of an Agent's Land Card cannot deal with land that stands in his or her name. It is strictly limited to acting for another in a conveyancing transaction.

By updating a Land Card of a specific type with another Transaction Authority, it is possible for the same Land Card to be used in circumstances that would ordinarily require a second Land Card.

The Land Card is an identification device but it also provides several other components that make it unique. Within the Land Card are eight components:

1. Storage - Storage (in the form of a suitable data storage device, such as a memory chip, magnetic strip or the like) allows the uploading of an Electronic Bank Receipt (see figures 12, 16A and 16B), details of a vendor's Transaction Authority, together with cancellation of the Transaction Authority upon dealing, into the Land Card. Although it would be expected that most users would apply for a Land Card of a single type, a few users may seek several Land Cards in order to play different roles. The Identification Service Agency is not expected to issue multiple Land Cards so that a party can play different roles. Instead, the Identification Service Agency will provide a means of uploading additional transaction limitations into the Land Card first issued. For example, a legal representative might hold an Agent's Land Card but wish to sell his or her own land. To do so, the legal representative will require the issue of a Vendor's Transaction Authority. This will be uploaded into the Agent's Land Card that the legal representative already has.

   Storage is also provided to permit the recording of any prior lodgement details that would cancel the operation of the Vendor's Transaction Authority.

   Storage is also required for details of the title reference of land nominated by a vendor as the Vendor's Link. Although a vendor may choose to place

only title reference details on the Land Card, all vendors are encouraged to place a full title search from Land Registry on the Land Card as the Vendor's Link. This search is placed on the Land Card at the time of its issue by an Identification Service Agency.

2. Expiry details - These consist of the date of issue and the latest date of Expiry. The Land Card also stores a means of comparing he latest date of expiry with the date contained in the metadata of any transaction for which it is being used for execution. A Land Card can be used for identification purposes for only a finite time after its capacity to enter into transactions has expired, so the Land Card also provides a means of comparing its remaining life for identification purposes with the records maintained by the issuing Identification Service Agency.

3. Transaction Authority - When a Land Card is issued for the use of a vendor, the Land Card contains a transaction authority. Although a vendor may have another Land Card in which the Vendor's Link pertains to the same land, the Land Registry will only accept the first lodgement of a transaction with the land by the vendor. Details of any lodging carried out using a Land Card are uploaded to the Land Card by the Settlement Manager cancelling the Transaction Authority for the person acting as vendor in the transaction.

4. Decryption and Encryption Engine - Because any encryption or decryption within the computer of a user would compromise the security of the transaction system, the Land Card itself performs all the encryption and decryption needed to transmit secure messages. All data that originates from or is dependent on other data in the Land Card is

transmitted from the Land Card to a user's computer in an encrypted form. All data passed from the Land Card to a user's computer is passed only after being encrypted on the Land Card.

5. Authorisation and Display of Any Funds due - As part of the settlement process (see figures 13A, 13B, 13C and 13D), a statement of funds received and paid within the transaction is uploaded onto the Land Card of all parties entitled to funds. This is an Electronic Bank Receipt and is outlined in more detail in figures 12, 16A and 16B. That part of the uploaded statement showing the name of the transaction, the total funds exchanged and the sum due to the holder of the Land Card are available for display on a computer after the Land Card and its supporting passphrase are used to initiate the display. As set out in figures 16A and 16B, once funds for a party entitled have been negotiated on the Electronic Bank Receipt, the entitlement of that person to funds from the transaction is cancelled on the Land Card of that person. This capacity to upload the Electronic Bank Receipt, display a subset of the information in the Electronic Bank Receipt pertaining to the holder of the Land Card and the process of cancellation of a party's entitlement is mediated by and on the Land Card.

6. Identification Key and ratification and encryption subkeys - Throughout the life of a Land Card, the Land Card can be used for identification purposes. Where the Land Card does not contain a Transaction Authority, it can also be used throughout its life for the purposes of legally signifying the holder's assent to data or documents. Where the Land Card contains a Transaction Authority, it can be used for the purposes of legally signifying the holder's assent to data or documents for the life of the Land

Card or until the transaction in which the holder is acting as vendor is lodged with Land Registry. The process of identification is mediated by and on the Land Card and transmitted in encrypted form to the data for which the holder of the Land Card is identifying himself or herself. The process of execution is mediated by and on the Land Card and transmitted in encrypted form to the data to which the holder of the Land Card is assenting or executing. The time of identification or execution and the party doing so are also transmitted to the metadata of the data concerned.

7. Name, Address, Date of Birth and Passphrase of the User - The processes of identification and execution depend upon encrypted data held within the Land Card that identify the holder of the Land Card to a high level of probability. These details not only provide part of the encryption seed but the name, address and date of birth of the party doing so are transmitted in encrypted form to the metadata of the data which the holder is executing or for which the holder is identifying himself or herself. The passphrase itself, chosen by the holder of the Land Card at the time that the Land Card was issued, has a minimum and maximum size and is designed to increase the keyspace of the encryption sufficiently to render its breaking impractical. Again, although the passphrase is entered on a computer keyboard, at no time will the passphrase enter the operating system of the host computer.

8. Parasitic Operating System - Anything entered within the operating system of a computer can be recovered in various ways and so threaten the security of the Land Card, so the Land Card also contains a secondary or parasitic operating system. Figure 17 is a schema of the parasitic operating system in relationship to

the Land Card and the user computer. Once uploaded to the Land Card's host computer (viz. the user computer of the Land Card holder) from the Land Card, the parasitic operating system creates a small memory space within the user computer that gives it control of the user computer's keyboard as well as sufficient memory to undertake passphrase entry for passing to the Land Card. The passphrase will be passed through this memory space to the Land Card, where the passphrase will be used to encrypt all data leaving the Land Card. As outlined in figure 18, this ensures that no information is decrypted or encrypted within the operating system of the host computer. Only when the information is "in the clear" is it passed from the parasitic operating system to the operating system of the host user computer.

When used for a transaction, the parasitic operating system also opens a single virtual port to the Single Data Entry Software or Settlement Software (depending on the circumstances) stored on the user's computer. Any entry using the keyboard is then passed through the parasitic memory space into the Land Card for encryption, decryption or validation. The first item to pass through that parasitic memory space in any part of a transaction requiring a Land Card is the passphrase that validates the use of the Land Card itself. Once validated by the passphrase, the Land Card is then used to manipulate all data entered by the keyboard.

Before passing data through the port into the single data entry software for transmission to the User Interface Manager for storage in the mode of storage chosen by the user, all data validated by the Land Card is encrypted using the decryption/encryption subkey contained on the Land Card. The encryption itself is done on the Land Card. The parasitic

operating system on the host system does not do this. The duties of the parasitic operating system on the host system are limited to maintaining a secure port to the memory space of the host computer's operating system and ensuring standard input and standard output connections to enable use of the identification key and ratification and encryption subkey contained on the Land Card.

Thus it is the Land Card where the passphrase will be used to encrypt all data leaving the Land Card. This is outlined in figure 17 and ensures that no information is decrypted or encrypted within the operating system of the host computer

For uploading for storage of data such as details of the Electronic Bank Receipt, the parasitic operating system receives encrypted transmission through the port between it and the host computer's operating system and passes the data to the Land Card for decryption and validation if needed or for storage on the Land Card.

When the data regarding an Electronic Bank Receipt must be downloaded for display at a negotiating bank, the process is undertaken in reverse. The Electronic Bank Receipt is firstly decrypted on the Land Card and then passed through an application also on the Land Card, which strips it of any details save that of the transaction identifier, the total sum and the details of the funds payable to the holder of the Land Card. These remaining details are then passed from the Land Card to the memory space of the host computer's operating system to an application that displays these details to a negotiating teller. The Electronic Bank Receipt remains stored intact on the Land Card.

D. Electronic Bank Receipt (see figures 12, 16A and 16B)

The Electronic Bank Receipt is a negotiable bank receipt. That is, it is a form of financial instrument in which one or more parties promise to pay money to two or more parties severally. That is, the obligation of a party to pay is mutually independent of the obligation of any other paying party and is discharged by a tender of the money in obligation to any one or more of the receiving parties up to the amount of the obligation. The capacity of any party receiving funds is only up to the amount payable to that party.

Subject to going stale, a negotiable bank receipt remains open and payable until all the paying parties have discharged their several obligations.

In an example where there is a cheque from A to B, a second cheque from C to D and a third cheque from E to F, there are two differences between a negotiable bank receipt and a cheque. The first difference is that there is only one instrument.

The second difference is that the obligations may not be discrete. In the above example of the three cheques, the total obligation of A is contained in his or her promise to pay B. In a negotiable bank receipt with three payees and three recipients, the total obligation of A may be greater that his or her obligation to B. It may be part of the obligation to C. Similarly, the obligation of E might be less than any total payment due to F.

In other words, the total amount of the obligations of the payees equal the payments due to the recipients but there is no necessary correlation between the individual obligations of a payee and payments due to any individual.

This concept of the financial instrument is useful in any

transaction where there are multiple obligations payable or delivery of multiple titles to goods or services in respect of a matter and multiple parties are owed payments from the same matter. It avoids the need of a central balancing account or multiple payment and redraw of cheques to balance out the payments against the obligation owed.

However, because the concept would, in a paper-based system, require one paper instrument that can be assigned like any other promissory note, it is clumsy. It would also be clumsy because, with multiple payees and one instrument, there would be difficulties with possession of the negotiable instrument.

When this concept is converted into an electronic context, however, it becomes both feasible and of great value.

Electronically, the financial instrument can be treated in the same way as a paper version of any financial instrument with one exception. An electronic environment permits a number of validated copies of the same receipt to be issued and negotiated independently of one another.

The electronic environment also enables validated copies of financial instrument to be electronically issued to several payees. Because of the electronic form, the validated copy of a financial instrument issued to a party can be limited to use by that party and by any party to whom it is negotiated. Once negotiated with a financial institution, that validated copy of a financial instrument can be cancelled, even though other validated copies of the financial instrument remain unnegotiated and no payment has been made on them.

E. Settlement (see figures 13A, 13B, 13C and 13D)

Settlement for electronic conveyancing or any form of this secure data management system is provided by the Settlement Manager. It enables the users to undertake safe and secure settlement in an asynchronous environment that enables them to work according to their own timetables.

After a user has completed all the parts of a transaction necessary before settlement can take place, the user must notify the User Interface Manager that he or she is ready to ratify the transaction. This commitment to settlement has no legal effect and can be reversed if necessary. It is merely an instruction to Land Trader to transfer the operation of all storage pointers from the User Interface Manager to the Settlement Manager module of Land Trader and retrieve an epitome of the transaction for ratification by the user.

At this stage, a user may choose to undertake an identity check of the other users in this transaction. This check, begun by pressing a button at the top of the client window, makes a computer-to-computer check online to the Identification Service Agency's computer and checks that the identities provided by the Land Card of these users are correct and match the other details in the Land Card. It will also ensure that the Land Cards used in the transaction remain valid. For a purchaser, this check ensures that the Land Card used by the vendor has not been used to settle the sale of this land previously.

The identity check is a voluntary step and one the Settlement Manager will not compel the parties to make.

If undertaken, the results of the identity check will appear in a dropdown box that validates the names and addresses of all the users who have identified themselves in the top window and demonstrates that the vendor's Land

Card has not been used to sell the land previously.

The Settlement Manager also offers another service that some users may choose to use if they wish. By pressing a button at the top of the client window, a purchaser or purchaser's mortgagee or indeed any user can undertake a check search. When pressed, this button remotely requests that the Land Registry provide a check of all dealings lodged with the Registrar over the previous one hundred and five days.

Although check searches are obtained prior to a settlement as part of paper-based conveyancing, they are seldom obtained as close to settlement as they ought to be. This capacity in the Settlement Manager offers users to a transaction an opportunity to improve the level of prudent conveyancing practice.

Again, this check search is a voluntary step and one the Settlement Manager will not compel users to make.

Each user then reviews those parts of the Coversheet that he or she controls or to which he or she has access. The Settlement Manager calls the requested parts of the Coversheet from the Transaction Locater, which then retrieves the information from the secure storage chosen by the users. Where a user is given access to data, it means that that user is also able to retrieve that data from the secure storage in which it is held, even though that access to that secure storage is otherwise controlled by the party controlling the data.

All users in a transaction have access to the data that is transmitted to the Land Registry at successful settlement but do not have access to the entire Coversheet. For example, the purchaser does not have access to the data, terms and conditions that go to make up the Authority to Sell that the vendor gave to the estate agent; nor does a

vendor have access to loan applications made by the purchaser.

Access to the data transmitted to the Land Registry by all parties is not a necessary requirement of electronic conveyancing or any embodiment of the secure data management system. Access to this data results from the nature of the transaction itself. A refusal of access to this data by a party to any other user will result in the transaction not proceeding.

Before settlement, most parties will have already checked the data and the terms and conditions to which they have access. Checking for most parties therefore involves reviewing that there has not been any further access to the part of the Coversheet in which they are interested since they checked the transaction. It will also involve the final checking of the adjustments that have been made to the balances payable by virtue of rate and tax adjustments. These adjustments appear in the epitome which in electronic conveyancing takes the form of a balance sheet.

It is common in paper-based settlements for parties to discuss and attempt to resolve problems that appear at the time of settlement. These problems should be much less common, because information committed to a Coversheet will be authenticated and validated, but the top of the client window of the Settlement Manager includes a tool for leaving a message for all or a specific party. If a message is left, the message will pop up over the top of the Settlement Manager's client window for the party sought.

Another tool for discussion and resolution of last minute difficulties is activated by a button that checks to see if the party or parties sought are connected to the Settlement Manager. If so, the screen for the Settlement

Manager splits in two, an upper and lower portion. From a party's point of view, the window on the computer screen is seen to divide into an upper and lower portion. In the bottom portion appear the words that he or she types. All the words typed by all the parties appear in the top portion. All words appearing in the top portion are transferred to the safe storage of all parties to the discussion at the completion of the transaction.

This tool is for conducting discussions between two or more of the parties to resolve issues with the settlement.

If a party is not online and connected to the Settlement Manager, this tool enables messages to be left for that party. The party or parties for whom the message is left is informed that there is a message waiting next time they enter the Settlement Manager. This message can then be inspected by the party and a reply made to the party leaving it by replying either by leaving a message or discussing it if the other party is online and connected to the Settlement Manager. If the party leaving the message is not online, a reply to the message can be left.

When satisfied, each party returns to the ratification of the transaction. Ratification is effected by each party using the ratification key in his or her Land Card to ratify the transaction.

It does not matter who ratifies first because, until all have ratified, nothing happens and settlement does not occur. Unlike paper-based conveyancing, this ratification is intended to demonstrate that each party is content with the transaction, as a whole. A ratification is conditional and does not signal settlement until all parties have ratified and until the agreed time for completion arrives.

Settlement occurs only when all parties have ratified and

the time for settlement arrives. Thus, both ratification by all parties and the arrival of the specified time are required for settlement. Settlement does not occur until both circumstances are present.

Every settlement has a time and date specified for completion. At the time and date specified, the settlement then takes place. No settlement occurs before the time and date specified, even if the parties have confirmed the transaction. As with paper-based conveyancing, parties can change the date and time of settlement but this requires the agreement of all parties to the settlement.

At the time of settlement specified by the parties and after ratification by the last of the parties, the Coversheet will lock. No further amendments, even if agreed by the parties, can be made to the Coversheet from that point on.

Only at that time specified does the Settlement Manager begin its checking and netting processes. If completed satisfactorily, lists of payments and the net position of the financial institutions involved are passed to the Financial Settlement Manager so that the interbank settlement can take place. After the Financial Settlement Manager notifies the Settlement Manager of successful interbank settlement the contents of the epitome that pertain to title to land are transmitted to the Land Registry, with details of the various executions by the parties for lodgement. Once the system operated by the Land Registry for its lodgement processes has verified the details and accepts the lodgement is settlement complete.

At the time of interbank settlement, immediately negotiable funds in an irrevocable form are transmitted to the accounts of the persons entitled to them. This include the stamp duty payable to State Revenue Office,

lodging fees payable to Land Registry and of course the funds required to discharge the mortgages, if any, and the balance of funds, after adjustments, to the vendor.

Where an electronic bank receipt is in use, the details of the financial instrument, embodied in electronic conveyancing as an electronic bank receipt are uploaded, after lodgement of data with Land Registry, to the Land Card of the parties entitled to receive funds. The parties entitled to receive funds are only able to access details of the funds to which he or she is entitled but is able to negotiate them immediately.

At conclusion of these processes, the Land Registry notifies the computer of the users in the transaction that a successful lodgement has occurred.
Where parties are not online, an acknowledgement is forwarded by the Land Registry at their stated email address.

This notification and its supporting email messages will provide details of the dealing numbers allocated to the transaction.

F. Locked File (see figures 14A and 14B)

In existing paper-based conveyancing systems, most vendors and purchasers do not attend settlement. Although it is possible for a vendor or purchaser to log on to Land Trader in order to review and ratify a transaction, it is probable that there will be a group of vendors and purchasers who do not wish to do so.

To accommodate this group, the present electronic conveyancing system includes a "Locked File" system. A Locked File contains the contents of a Coversheet applicable to the user wishing to use it and which have been executed by that user by means of his or her Land

Card. A user prepares a Locked File by inspecting the applicable parts of a Coversheet and then requesting that the Single Data Entry Software clone those parts. The Single Data Entry Software does so and marks the clone with the date and time of cloning. Stored at first in the Single Data Entry Software on a user's computer, the contents of this clone are then not added to storage in the ordinary way but kept separately on the Single Data Entry Software. The clone's contents may be altered in any way the party chooses. When satisfied with the final form of the Coversheet clone, the user ratifies the clone using that user's Land Card. In this case, the clone is encrypted using the Land Card of the individual and can be downloaded onto any portable storage he or she may choose. The party may also leave the clone stored in the Single Data Entry Software. At settlement, this locked file is downloaded to the Settlement Software on any user's computer and hence is matched by the Settlement Software against the Coversheet details that are to be transmitted to the Land Registry. If there is an exact match of the details between the clone and the final form of the Coversheet, the Settlement Manager incorporates the earlier execution by the party of the Locked File as that party's ratification of the epitome of the Coversheet for settlement purposes. In that event, the Settlement Manager proceeds to settlement as if the final epitome of the Coversheet had been ratified by the absent party.

If there is an exact match of the details between those parts of the clone that are completed and the final form of the Coversheet but parts of the completed clone are left blank, the party providing the Locked File is deemed to have agreed that those parts of the completed clone left blank are to be the equivalent parts of the final form of the Coversheet.

Any discrepancy between the clone/amended Coversheet (corresponding to the Locked File) and the final data of

the Coversheet, as retrieved from storage to be transmitted as an epitome to the Land Registry, results in the settlement aborting.

G. Particular Terms not otherwise defined

1. Identification Service Agency:
The Identification Service Agencies are external organisations, who provide the identification and authentication services. They may be appointed in any preferred manner, such as by seeking tenders from organisations wishing to fulfil this function.

Such a tender need not be exclusive. However, if the provision of these services is to be undertaken by more than one Identification Service Agency, the Land Cards issued by one Agent are able to be used with the electronic conveyancing system even when other parties to the particular transaction are using Land Cards issued by other Agents.

An Identification Service Agency provides these identification and authentication services independently of the Registrar of Lands or any user in a transaction. However, the Agent is preferably required to provide regular audits and other measures of quality assurance for the Registrar's purposes. The Agent is also preferably required to allow the Registrar full access, and to allow the Registrar to conduct these audits and other measures of quality assurance himself.

It is also clearly preferable that the agreement to provide identification and authentication services, and thereby be appointed an Identification Service Agency, should be between the prospective Identification Service Agency and the Registrar.

In the event of a Land Card being issued in error or issued to a person other than the applicant who applied for that Land Card, an Identification Service Agency will be expected to demonstrate that it had taken all reasonable steps to identify the applicant and issue the Land Card correctly. A failure to discharge that burden of proof will result in an Identification Service Agency being liable to the Registrar for any money that he pays pursuant to the relevant local statutory provisions (such as, in the example of the State of Victoria, Australia, sections 109, 110 and 111 of the *Transfer of Land Act 1958*).

In the event of a Land Card being issued fraudulently or used for the purposes of fraud, an Identification Service Agency will be expected to demonstrate that it had taken all reasonable steps to identify the applicant and issue the Land Card correctly. A failure to discharge that burden of proof will result in an Identification Service Agency being liable to the Registrar for any money that he pays pursuant to the relevant local statutory provisions (again, such as - in the State of Victoria, Australia - sections 109, 110 and 111 of the *Transfer of Land Act 1958*).

2. Identification Key:

The Identification Key is contained on the Land Card, and uses the personal details in conjunction with a Land Card's passphrase to allow a user to identify himself or herself. A ratification subkey also contained on the Land Card enables a user to enter into binding legal agreements using the Land Card

3. Settlement Software:

The Settlement Software enables a party to review and ratify a transaction conveniently and securely, and also provides a set of tools for remotely undertaking a check title search, a identification check and

typed discussions with all the parties to a transaction or specific parties chosen by the party. The Settlement Software can also leave a message for other parties to the transaction to read as well as providing details of successful and unsuccessful lodgements and settlements. The Settlement Software also provides the virtual private network interface to the Settlement Manager and transfers details of an electronic financial instrument, in this embodiment of the secure data management system using electronic conveyancing called the Electronic Bank Receipts, to the Land Card of receiving parties via a Parasitic Operating System used by the Land Card.

4. Single Data Entry Software:

The Single Data Entry Software enables a user to conveniently and securely create a Coversheet and enter data in that Coversheet for a transaction in the structure and form required for the jurisdiction in which the transaction is to be lodged. It provides the submission and retrieval mechanism to the mode of secure storage chosen by the user and accepts both the identification of an individual and execution of binding legal agreements by that individual using its interface to the parasitic operating system of the Land Card. This software is designed for those who undertake single or limited conveyancing tasks or to casual users. It is anticipated that conveyancing professionals and financial institutions would employ their own interfaces to the secure data management system of this embodiment. The presentation and transport layers and their toolboxes are intended to assist them in the development of such interfaces.

In essence, Single Data Entry Software is the interface up to the time of settlement between a party and the Coversheet for the transaction.

5. Authorization and Display Processor:
This component of the Land Card authorizes, enables and verifies the uplift of the Electronic Bank Receipt and its display and cancellation when negotiated.

It should be noted, however, that modifications within the spirit and scope of the invention may readily be effected by a person skilled in the art. Consequently, it is to be understood that the invention is not limited to the particular embodiment described by way of example hereinabove.

CLAIMS:

1. An identification and authentication device for a user to identify himself or herself and to execute documents or transactions, comprising:

identification means for identifying said user;

transaction authority means, for indicating the type or types of transaction that said user can execute by means of said device; and

digital storage capacity;

wherein said device is operable to identify said user, and by said user to execute transactions of the type or types specified by said transaction authority means.

2. A device as claimed in claim 1, wherein said transaction authority means comprises transaction authority information stored in said digital storage capacity.

3. A device as claimed in either claim 1 or 2, wherein said digital storage capacity comprises a computer disk drive or merely a surface of the device bearing the relevant information in bar code or other comparable format.

4. A device as claimed in any one of the preceding claims, wherein said device is operable to expire after a predetermined period.

5. A device as claimed in any one of the preceding claims, wherein said identification means is stored in said digital storage capacity.

5. A device as claimed in any one of the preceding claims, wherein said device is operable to download and store data pertaining to said documents or transaction.

6. A device as claimed in any one of the preceding

claims, wherein said device is operable to store details of an electronic financial instrument associated with said transaction.

7. A device as claimed in any one of the preceding claims, wherein said transaction authority means is operable to authorize a predetermined type or types of transaction only when a password has been provided to said device or in association with said transaction.

8. A device as claimed in any one of the preceding claims, wherein said transaction authority means designates that said device is for use by a vendor or member of a group who owns, controls or possesses the title to goods or services where goods include any rights in land.

9. A device as claimed in claim 8, wherein said device is operable to retain information pertaining to that which said vendor or member of said group intends to sell assign, lease or otherwise limit his or her right to said goods or services.

10. A device as claimed in claim 9, wherein said device is provided with said information pertaining to that which said vendor or member of said group intends to sell assign, lease or otherwise limit his or her right to said goods or services when the device is issued only.

11. A device as claimed in any one of claims 1 to 7, wherein said transaction authority means designates that said device is for use by a purchaser or a member of another discrete group.

12. A device as claimed in any one of claims 1 to 7, wherein said transaction authority means designates that said device is for use by an agent of another party whether or not this user is an agent of the said groups.

13. A device as claimed in any one of the preceding claims, wherein said device is a computer peripheral device operable to communicate digitally with a user computer.

14. A device as claimed in any one of the preceding claims, including a secondary operating system and operable to load digital data into a user computer having an input means and an operating system, by:

arranging said user computer and said identification and authentication device to be in data communication with one another;

transferring said secondary operating system from said identification and authentication device to said user computer;

running said secondary operating system on said user computer such that control of said input means is appropriated by said secondary operating system; and

mediating at least some communication between said user computer and said identification and authentication device by means of said secondary operating system;

whereby said at least some communication is performed other than by means of said operating system of said user computer.

15. A device as claimed in claim 14, wherein said device is operable to process digital data located on said device, whereby said processed digital data is subsequently transferred to said user computer, and said processing of said digital data is performed by said device rather than by said operating system of said user computer.

16. A device as claimed in either claim 14 or 15, wherein said user computer is operable to receive said digital data by means of said input means after said secondary

operating system has appropriated control of said input means, whereby said digital data is subsequently transferred to said identification and authentication device.

17. A device as claimed in any one of claim 14 to 16, wherein secondary operating system is operable to create a memory space within said user computer to gain control of said input means.

18. A device as claimed in any one of claim 14 to 17, wherein said secondary operating system is operable to mediate input of a password or passphrase, to pass said password or passphrase to said identification and authentication device, and to process said digital data according to said password or passphrase.

19. A device as claimed in claim 18, wherein said processing of said digital data comprises manipulating said digital data, screening said digital data or both manipulating and screening said digital data.

20. An electronic transaction system for conducting a transaction over a computer network, comprising:

submission means for allowing any of one or more users to submit respective user information pertaining to said transaction, the sum of said respective user information at any time constituting transaction information;

storage means for storing and retrieving said information; and

execution means in the form of an identification and authentication device as claimed in any one of the preceding claims, for allowing any of said users to execute or indicate assent to at least some of said transaction information;

wherein said transaction information, when complete, includes all information required to conduct

said transaction, and whereby any of said users can submit, inspect and execute or assent to any part of said transaction information required for said transaction to be completed.

21. A system as claimed in claim 20, wherein said submission means comprises software portions, software portions stored on a computer readable medium, computer hardware, or a combination of hardware and software.

22. A system as claimed in claim 20, including means for retrieving, or for retrieving and displaying, said transaction information to any of said users.

23. A system as claimed in claim 20, including means for retrieving, or for retrieving and displaying, said transaction information to any of said users in a single coherent form, whereby said transaction information appears to comprise a single document or computer file.

24. A system as claimed in claim 20, wherein said storage means comprises software portions for controlling the storage and retrieval of the respective user information.

25. A system as claimed in claim 20, including one or more computer readable and writeable media for storing the respective user information, said storage means comprising software portions for controlling the storage and retrieval of the respective user information and said one or more computer readable and writeable media.

26. A system as claimed in claim 20, including pointer storage means for the storage of information storage pointers, whereby said system is operable to maintain in said pointer storage means a pointer to the location of each item of user information stored by said storage means.

27. A system as claimed in any one of claims 20 to 26, including an electronic financial instrument comprising:

digital data packets encoding information concerning one or more payments pertaining to a transaction;

digital storage means for storing some or all of said data packets; and

display means for displaying some or all of said information.

28. A system as claimed in claim 27, wherein said instrument is operable to display said information to a user only upon presentation by said user of suitable identification.

29. A system as claimed in claim 27, wherein said instrument is operable to display to said user only that part of said information pertaining to said user.

30. A system as claimed in claim 27, wherein said instrument is operable to display to said user only that a summary of said information in which net payments or obligations to or from said user are indicated.

31. A system as claimed in any one of claims 27 to 30, wherein said electronic instrument is a negotiable financial instrument in the form of a bill of lading, an insurance bond, a bearer bond or a banker's warrant.

32. A system as claimed in any one of claims 27 to 30, wherein said electronic instrument is a negotiable financial instrument operable to function as an electronic bank receipt.

33. A system as claimed in any one of claims 27 to 30, wherein said instrument is storable on a portable device.

34. A system as claimed in any one of claims 20 to 33,

including a secure data management method means comprising:

retrieval means for retrieving information pertaining to a transaction from one or more digital storage means;

inspection means for inspecting said information to determine whether said information includes or has been associated with suitable ratification data indicative of the ratification of said information or respective parts of said information by respective parties to said transaction; and

ratification means for flagging said transaction as ready for settlement if said ratification data is located.

35. A system as claimed in claim 34, wherein said transaction settlement means is operable to deem said transaction as ready for settlement at a predetermined time.

36. A system as claimed in either claim 34 or 35, wherein said inspection means comprises computing means.

37. A system as claimed in any one of claims 20 to 36, wherein said system is operable:

by a respective party or a user who has not submitted user information to a transaction to copy information pertaining to said party or any information to which said user has access and to said transaction from a computer network onto a user computer of said party or a user who has not submitted user information;

by said party or a user who has not submitted user information to augment or amend said downloaded information to form amended information;

by said party or a user who has not submitted user information to execute or assent to said amended information so that said amended information includes execution data; and

to compare said amended information with said information and deem those parts of said amended information that are consistent with said information to have been executed or assented to.

38. A system as claimed in any one of claims 20 to 37, wherein said system is operable to augment said downloaded information with the time of downloading.

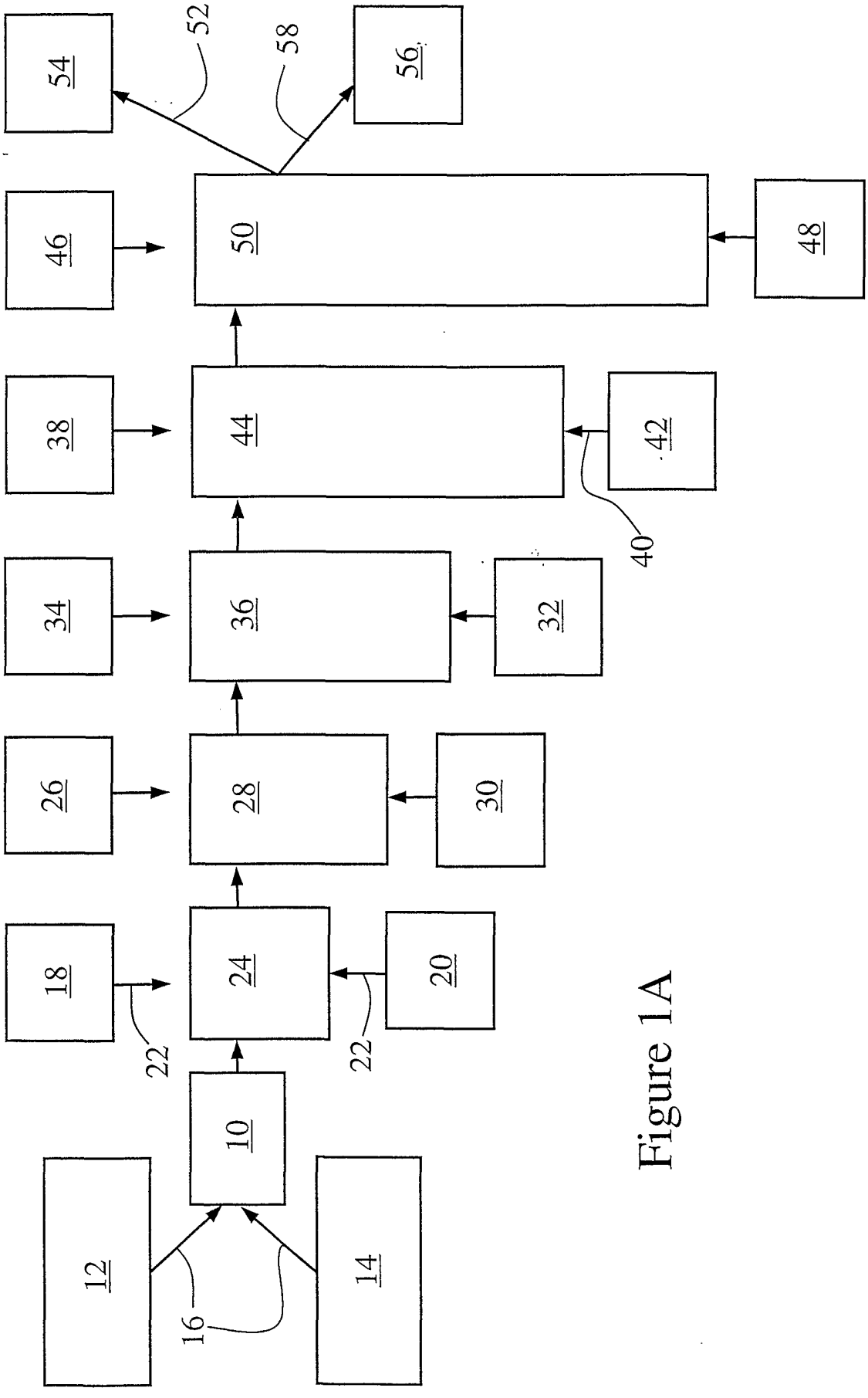

54
52
58
56
46
50
48
38
44
42
40
34
36
32
26
28
30
18
24
20
22
22
10
12
16
14

Figure 1A

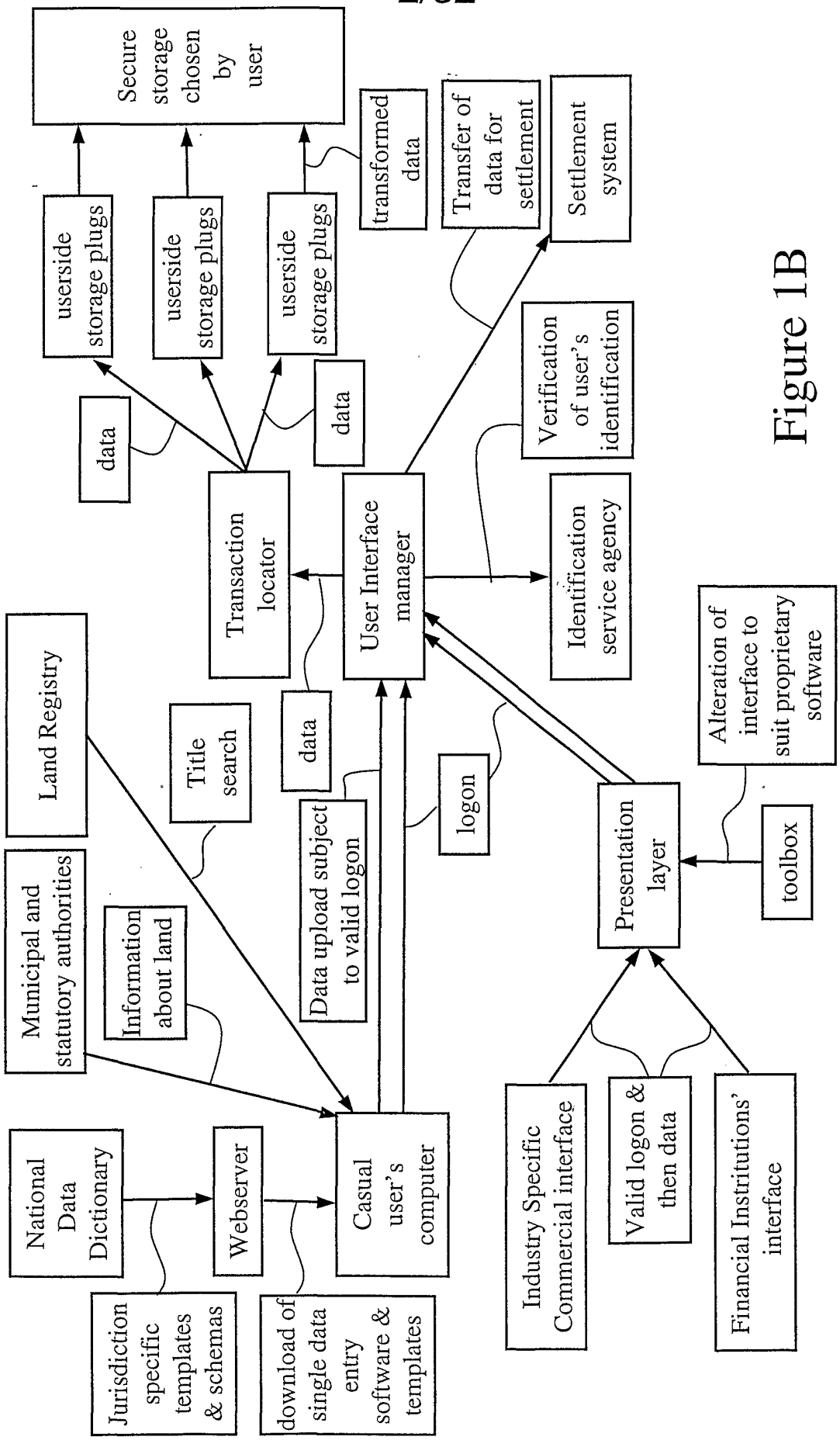

Secure storage chosen by user
userside storage plugs
userside storage plugs
userside storage plugs
transformed data
Transfer of data for settlement
Settlement system
data
data
Verification of user's identification
Transaction locator
User Interface manager
Identification service agency
Land Registry
Title search
data
Alteration of interface to suit proprietary software
logon
Municipal and statutory authorities
Information about land
Data upload subject to valid logon
Presentation layer
toolbox
National Data Dictionary
Webserver
Casual user's computer
Industry Specific Commercial interface
Valid logon & then data
Financial Institutions' interface
Jurisdiction specific templates & schemas
download of single data entry software & templates

Figure 1B

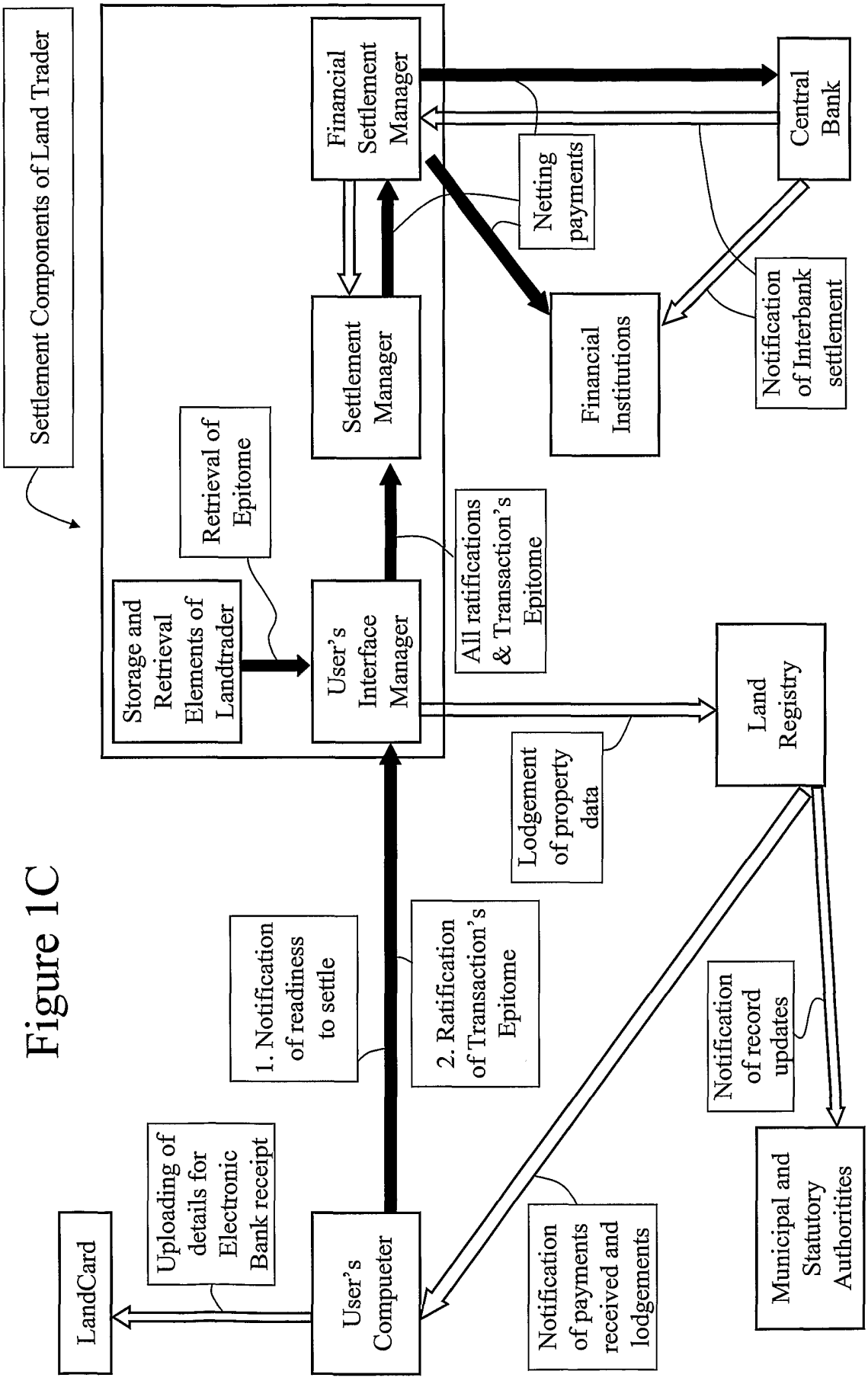

Settlement Components of Land Trader
Financial Settlement Manager
Central Bank
Netting payments
Settlement Manager
Financial Institutions
Notification of Interbank settlement
Retrieval of Epitome
Storage and Retrieval Elements of Landtrader
User's Interface Manager
All ratifications & Transaction's Epitome
Land Registry
Lodgement of property data
1. Notification of readiness to settle
2. Ratification of Transaction's Epitome
Notification of record updates
Uploading of details for Electronic Bank receipt
LandCard
User's Compueter
Notification of payments received and lodgements
Municipal and Statutory Authoritites

Figure 1C

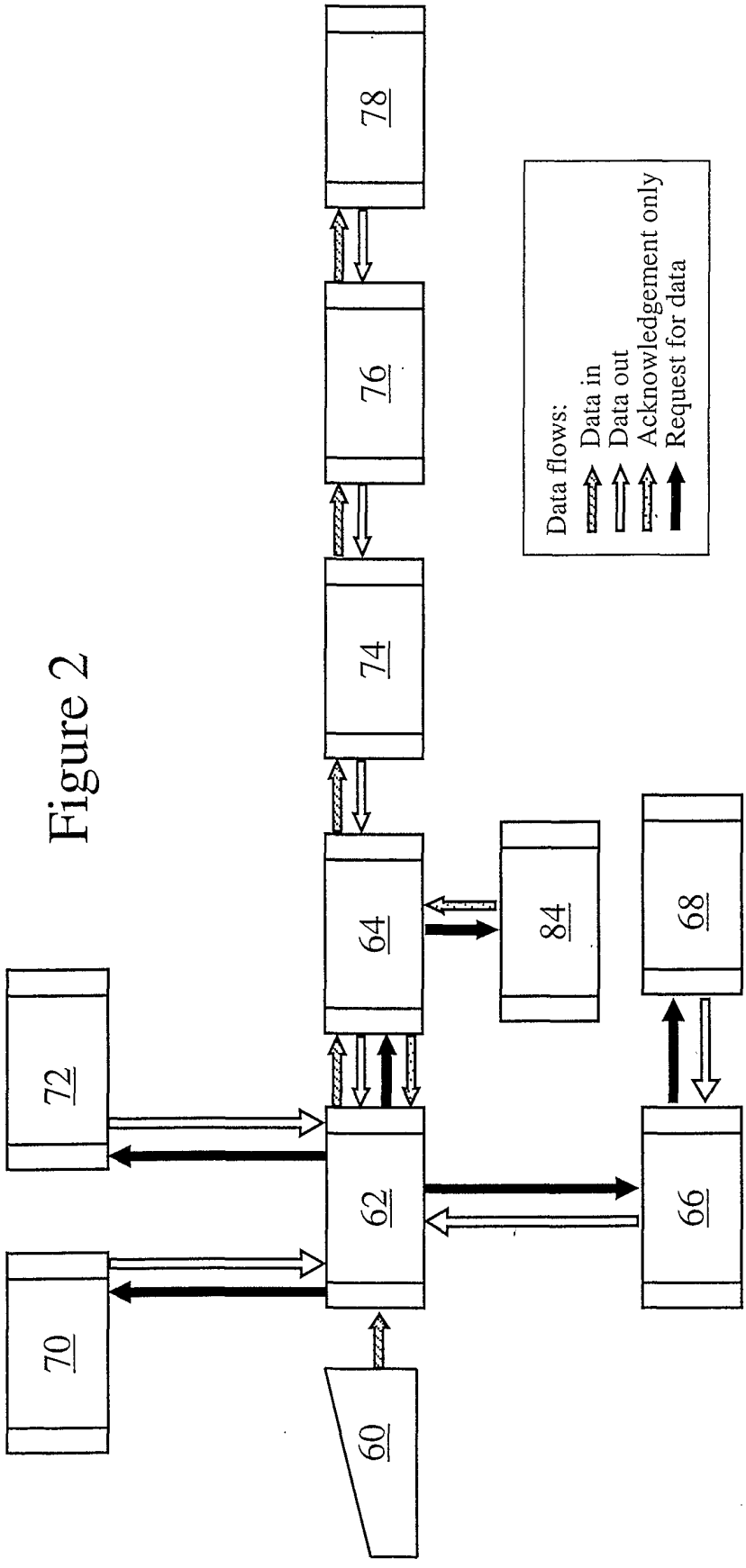

78
76
74
64
84
68
72
62
66
70
60
Data flows:
Data in
Data out
Acknowledgement only
Request for data

Figure 2

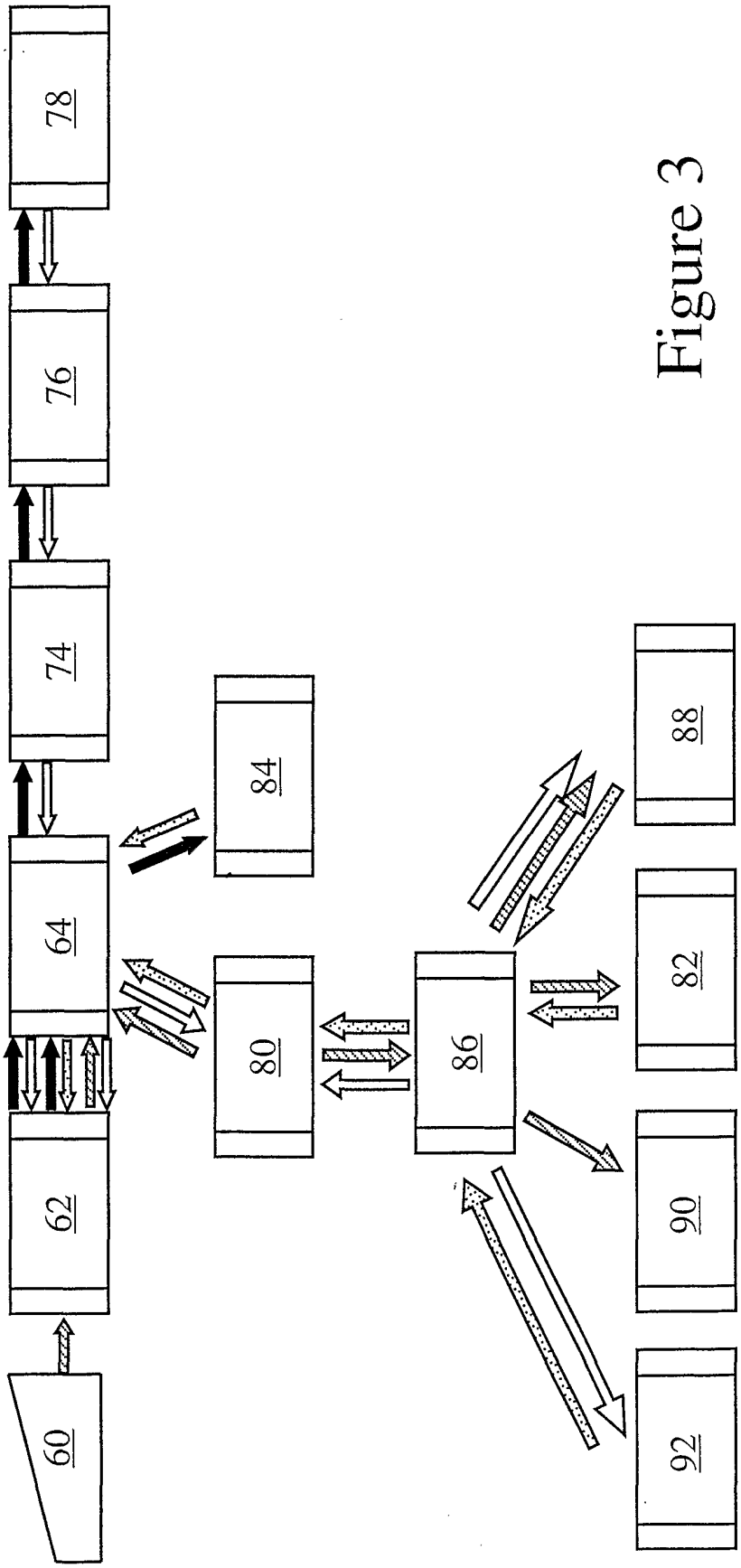


Figure 3

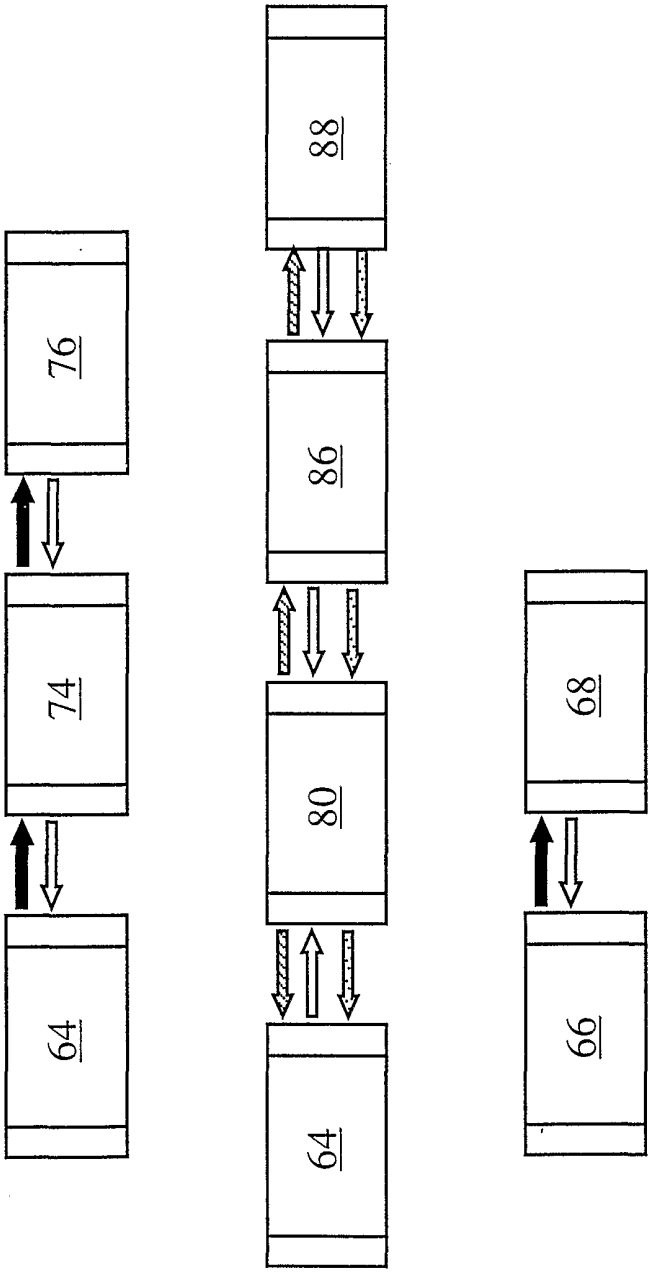


Figure 4

Figure 5

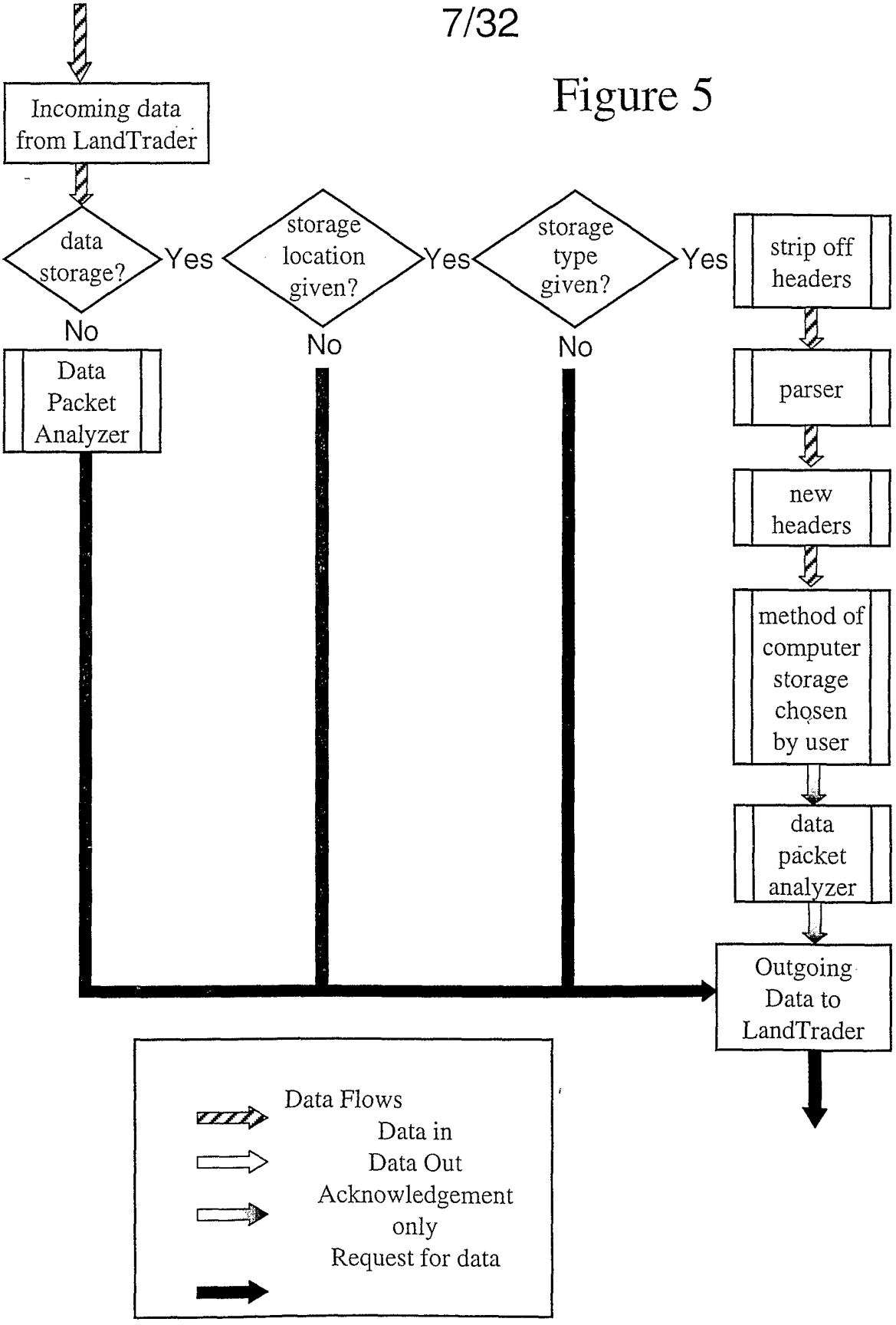
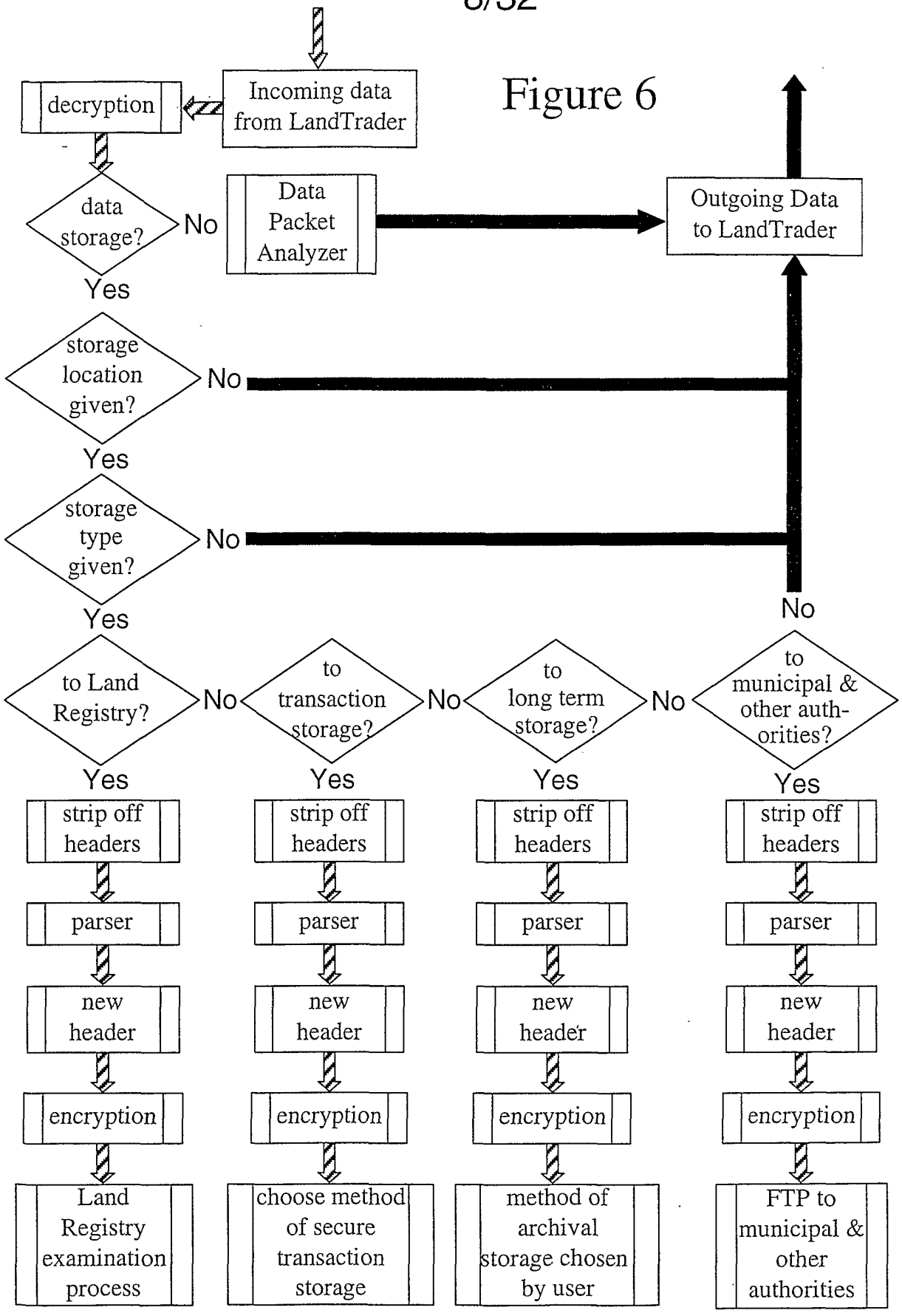

Incoming data from LandTrader
data storage?
Yes
No
Data Packet Analyzer
storage location given?
Yes
No
storage type given?
Yes
No
strip off headers
parser
new headers
method of computer storage chosen by user
data packet analyzer
Outgoing Data to LandTrader
Data Flows
Data in
Data Out
Acknowledgement only
Request for data

Figure 6


Incoming data from LandTrader
decryption
data storage?
No
Data Packet Analyzer
Outgoing Data to LandTrader
Yes
storage location given?
No
Yes
storage type given?
No
Yes
to Land Registry?
No
to transaction storage?
No
to long term storage?
No
to municipal & other auth-orities?
Yes
Yes
Yes
Yes
strip off headers
parser
new header
encryption
Land Registry examination process
strip off headers
parser
new header
encryption
choose method of secure transaction storage
strip off headers
parser
new header
encryption
method of archival storage chosen by user
strip off headers
parser
new header
encryption
FTP to municipal & other authorities

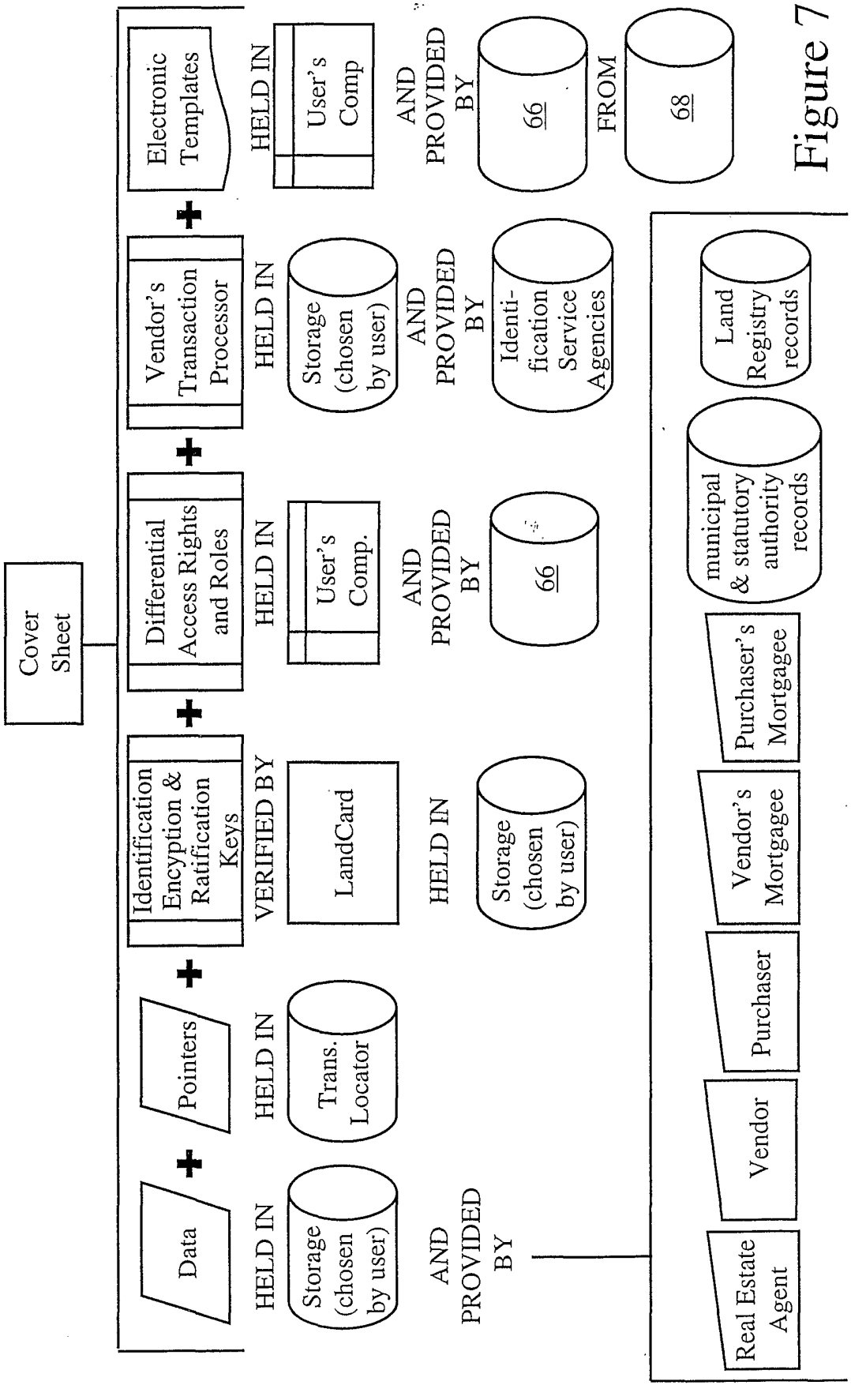

Cover Sheet
Data
Pointers
Identification Encyption & Ratification Keys
Differential Access Rights and Roles
Vendor's Transaction Processor
Electronic Templates
HELD IN
Storage (chosen by user)
HELD IN
Trans. Locator
VERIFIED BY
LandCard
HELD IN
User's Comp.
HELD IN
Storage (chosen by user)
AND PROVIDED BY
Storage (chosen by user)
AND PROVIDED BY
66
AND PROVIDED BY
Identi-fication Service Agencies
AND PROVIDED BY
66
HELD IN
User's Comp
AND PROVIDED BY
66
FROM
68
Real Estate Agent
Vendor
Purchaser
Vendor's Mortgagee
Purchaser's Mortgagee
municipal & statutory authority records
Land Registry records

Figure 7

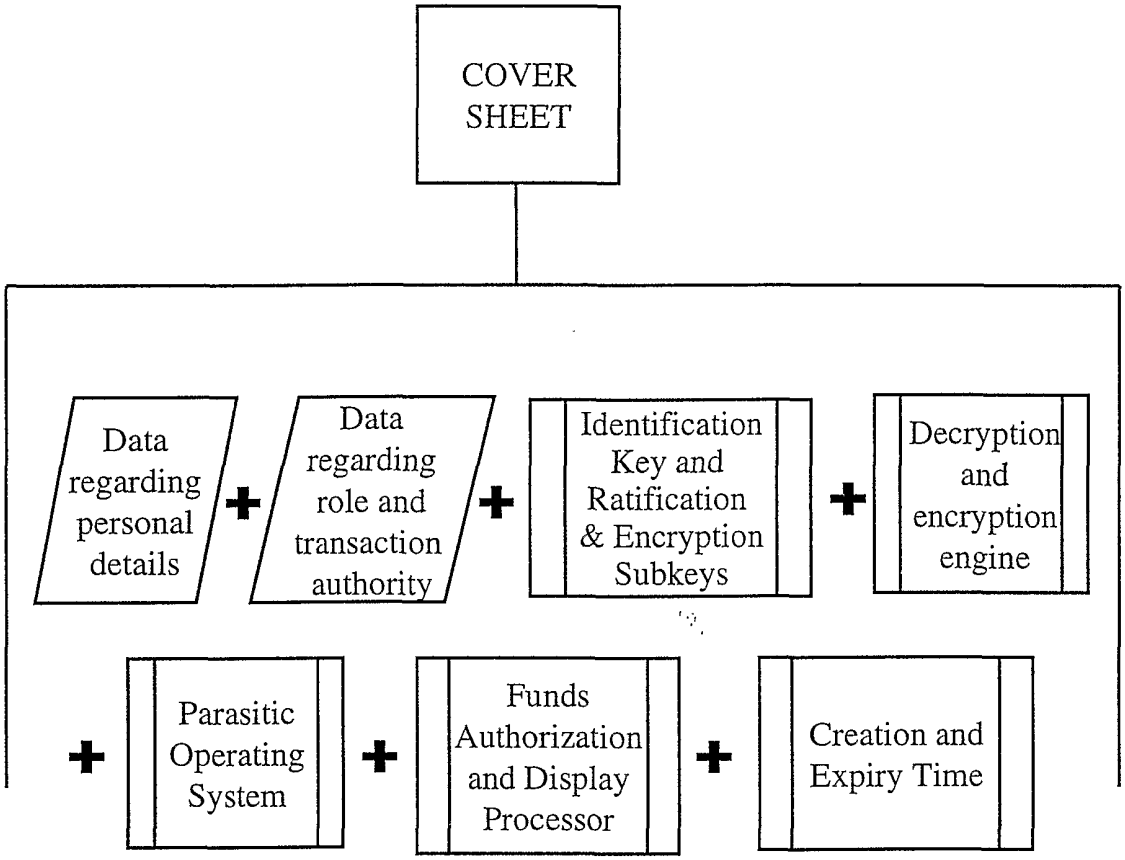

COVER SHEET
Data regarding personal details
Data regarding role and transaction authority
Identification Key and Ratification & Encryption Subkeys
Decryption and encryption engine
Parasitic Operating System
Funds Authorization and Display Processor
Creation and Expiry Time

Figure 8

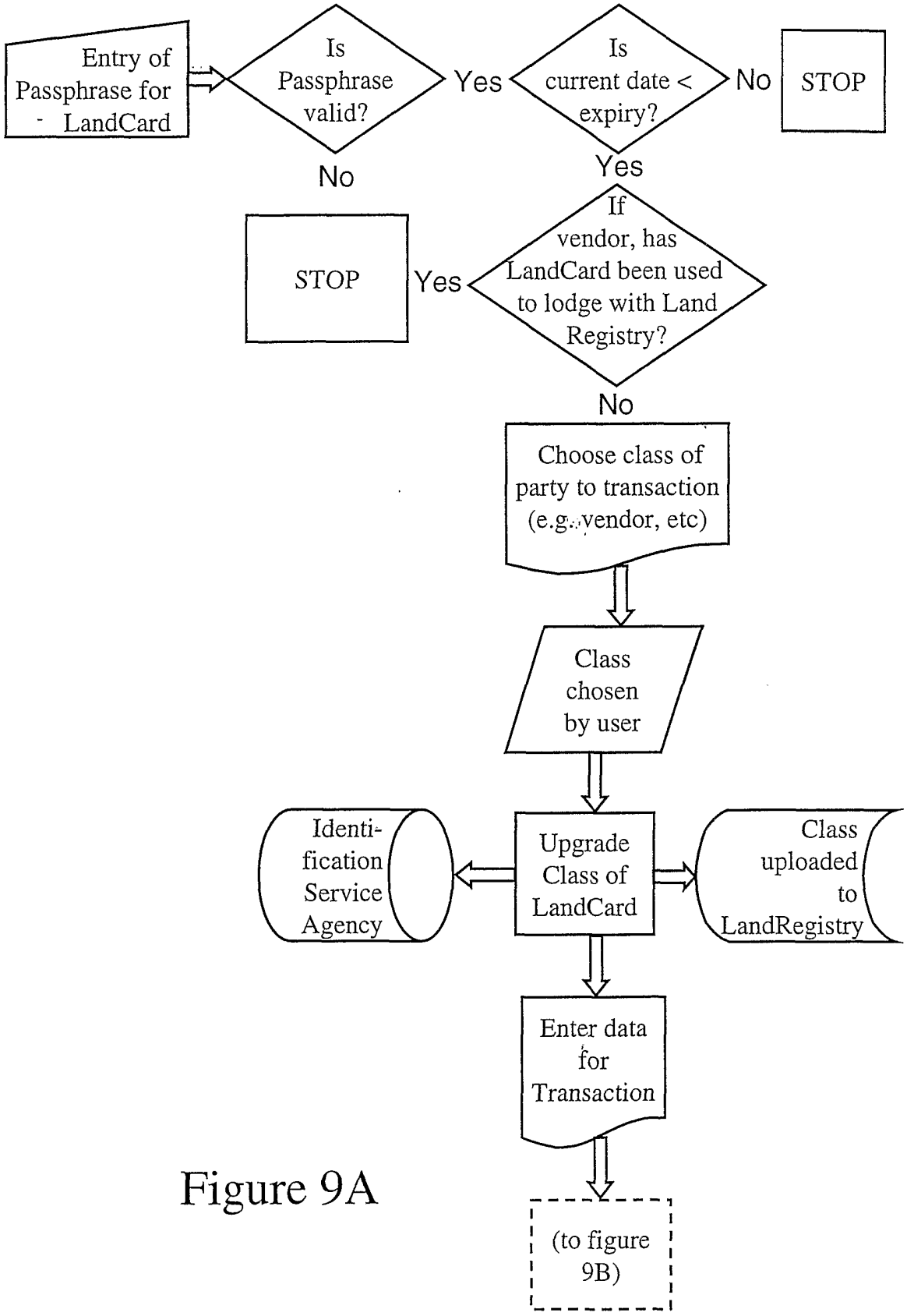

Entry of Passphrase for LandCard
Is Passphrase valid?
Yes
Is current date < expiry?
No
STOP
No
Yes
STOP
Yes
If vendor, has LandCard been used to lodge with Land Registry?
No
Choose class of party to transaction (e.g. vendor, etc)
Class chosen by user
Identi-fication Service Agency
Upgrade Class of LandCard
Class uploaded to LandRegistry
Enter data for Transaction
(to figure 9B)

Figure 9A

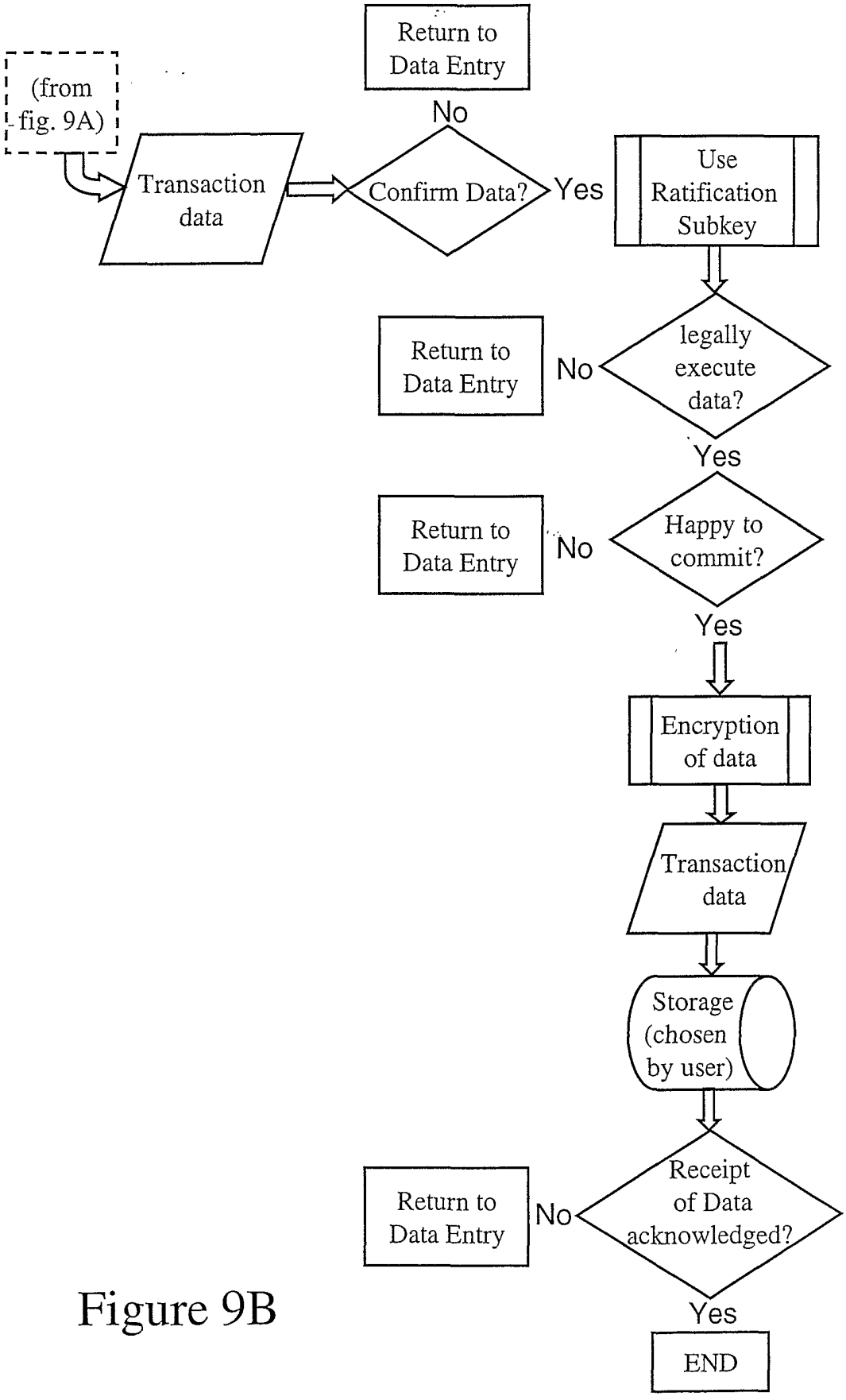

Return to Data Entry
(from fig. 9A)
No
Transaction data
Confirm Data?
Yes
Use Ratification Subkey
Return to Data Entry
No
legally execute data?
Yes
Return to Data Entry
No
Happy to commit?
Yes
Encryption of data
Transaction data
Storage (chosen by user)
Return to Data Entry
No
Receipt of Data acknowledged?
Yes
END

Figure 9B

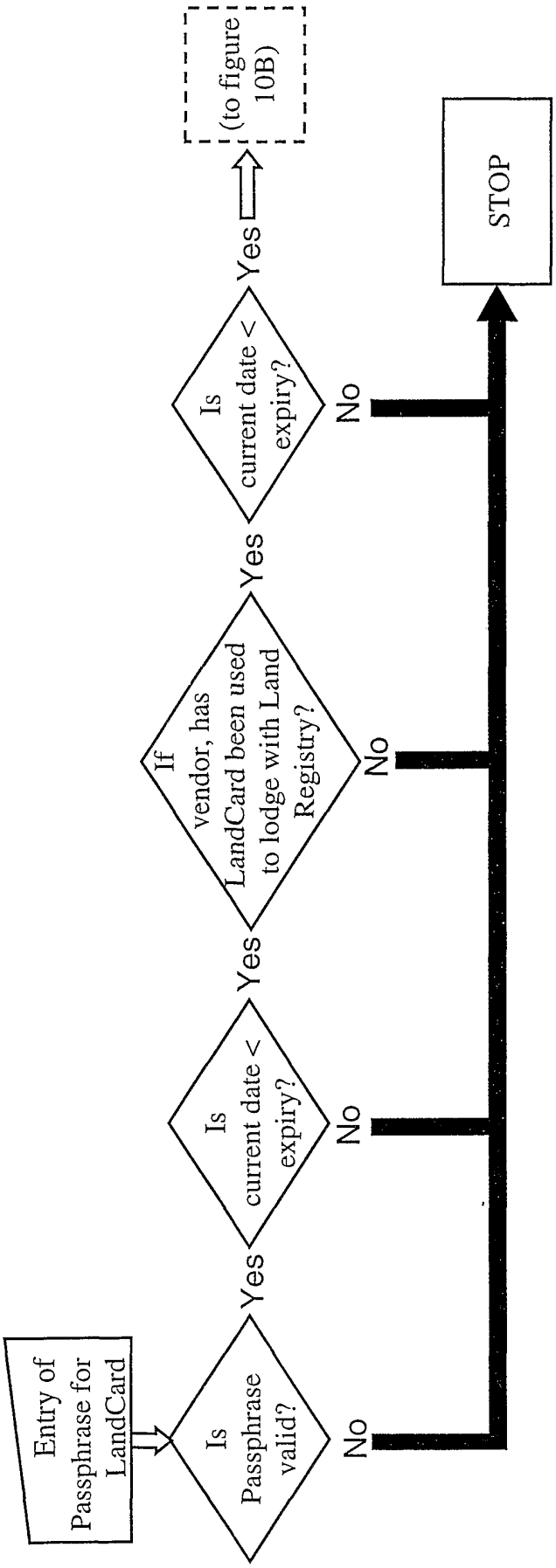

Entry of Passphrase for LandCard
Is Passphrase valid?
No
Yes
Is current date < expiry?
No
Yes
If vendor, has LandCard been used to lodge with Land Registry?
No
Yes
Is current date < expiry?
No
Yes
(to figure 10B)
STOP

Figure 10A

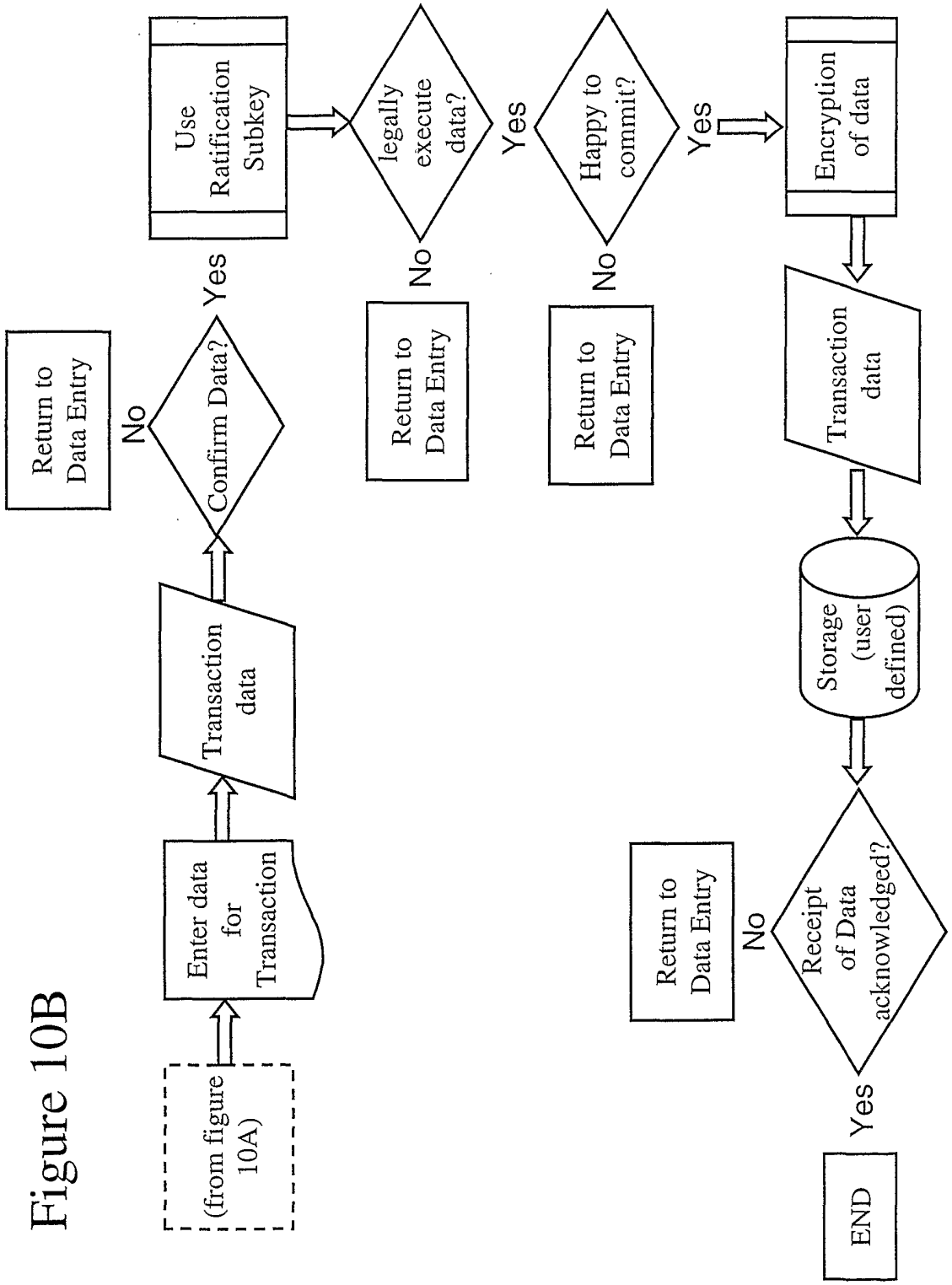

(from figure 10A)
Enter data for Transaction
Transaction data
Confirm Data?
No
Yes
Return to Data Entry
Use Ratification Subkey
legally execute data?
No
Yes
Return to Data Entry
Happy to commit?
No
Yes
Return to Data Entry
Encryption of data
Transaction data
Storage (user defined)
Receipt of Data acknowledged?
No
Yes
Return to Data Entry
END

Figure 10B

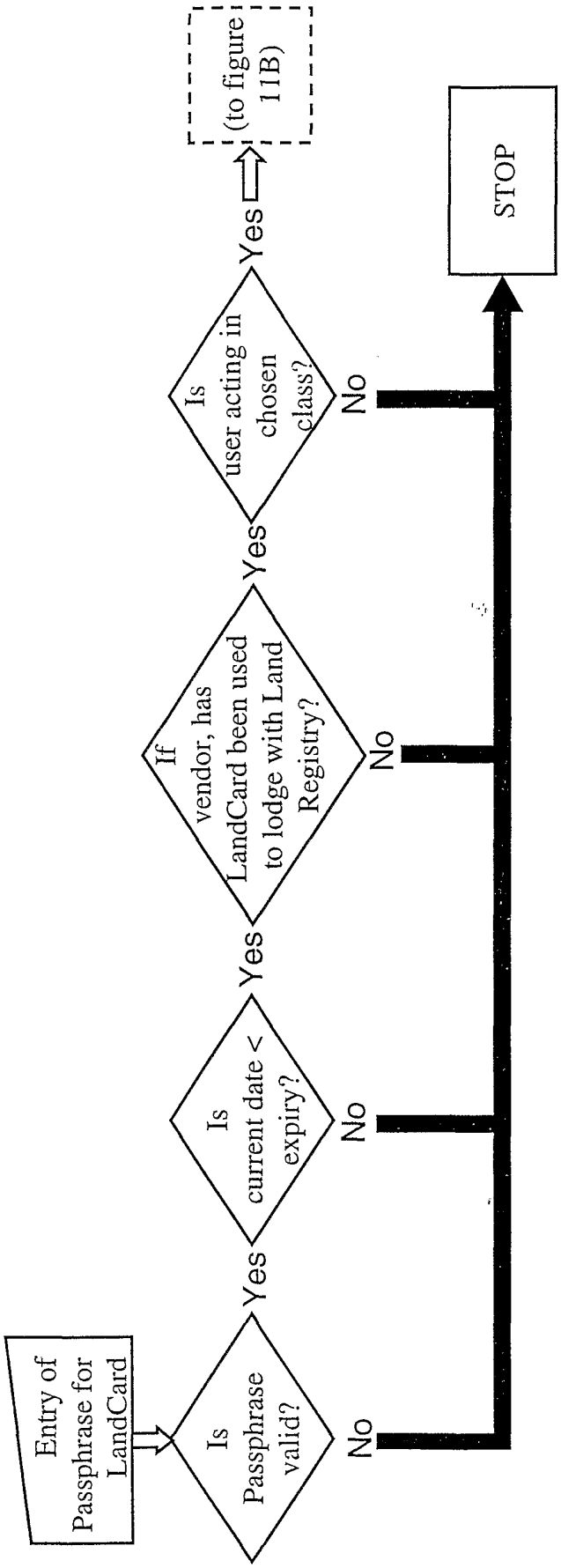

Entry of Passphrase for LandCard
Is Passphrase valid?
Yes
No
Is current date < expiry?
Yes
No
If vendor, has LandCard been used to lodge with Land Registry?
Yes
No
Is user acting in chosen class?
Yes
No
(to figure 11B)
STOP

Figure 11A

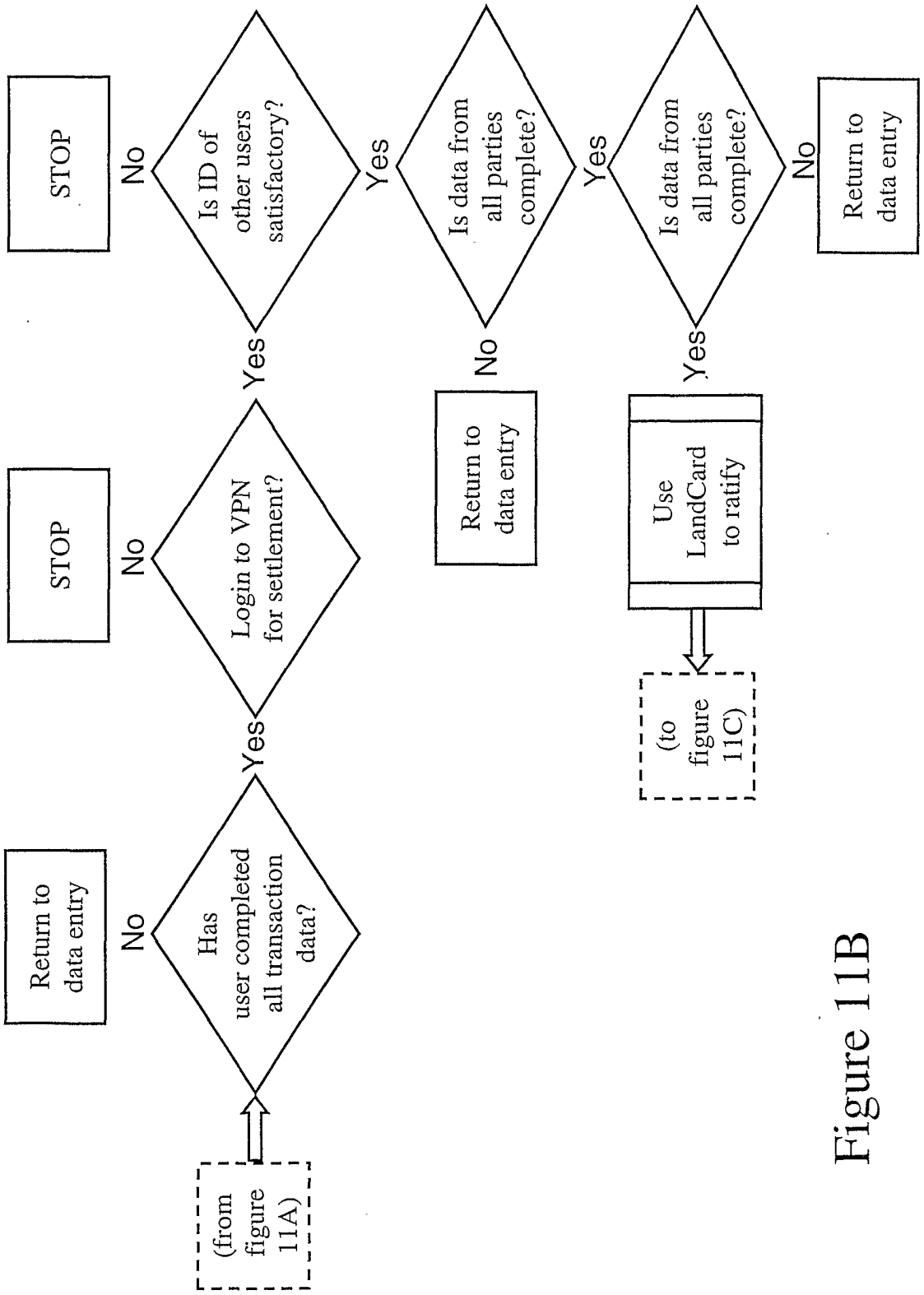
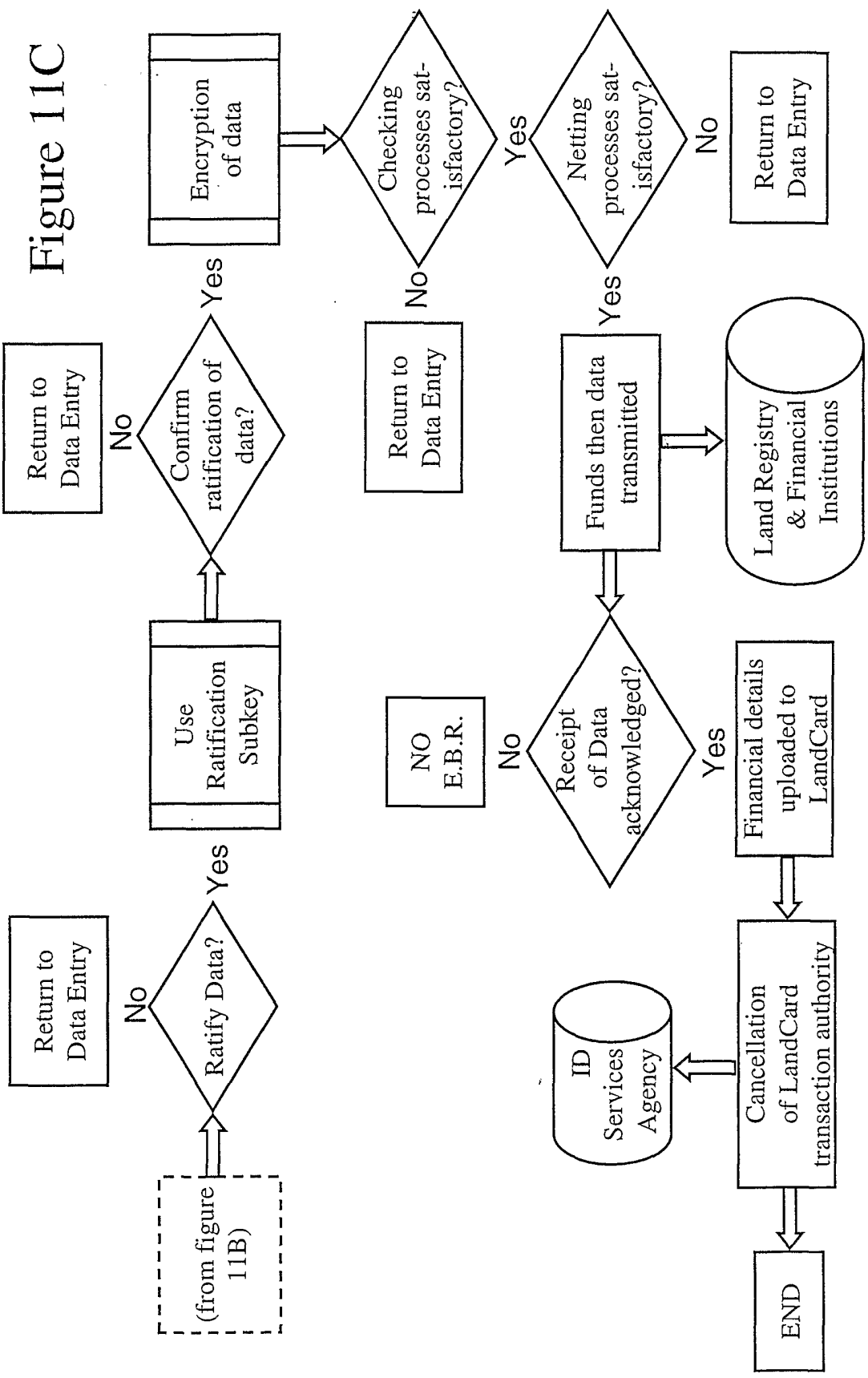

(from figure 11A)
Has user completed all transaction data?
No
Return to data entry
Yes
Login to VPN for settlement?
No
STOP
Yes
Is ID of other users satisfactory?
No
STOP
Yes
Is data from all parties complete?
No
Return to data entry
Yes
Use LandCard to ratify
(to figure 11C)
Is data from all parties complete?
No
Return to data entry
Yes

Figure 11B

Figure 11C


(from figure 11B)
Ratify Data?
No
Yes
Return to Data Entry
Use Ratification Subkey
Confirm ratification of data?
No
Yes
Return to Data Entry
Encryption of data
Checking processes satisfactory?
No
Yes
Return to Data Entry
NO E.B.R.
Receipt of Data acknowledged?
No
Yes
Funds then data transmitted
Yes
Netting processes satisfactory?
No
Return to Data Entry
Land Registry & Financial Institutions
Financial details uploaded to LandCard
ID Services Agency
Cancellation of LandCard transaction authority
END

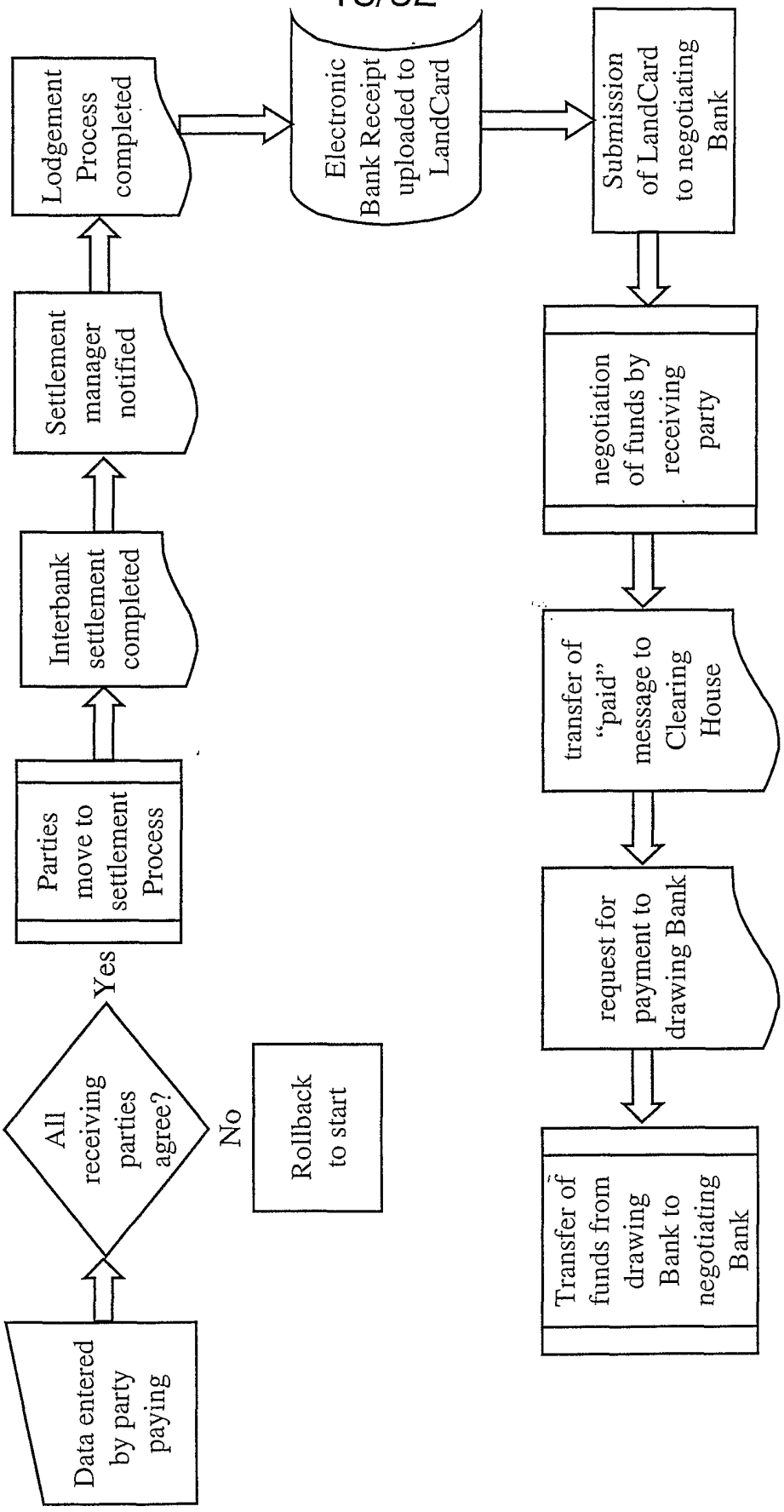

Data entered by party paying
All receiving parties agree?
Yes
No
Rollback to start
Parties move to settlement Process
Interbank settlement completed
Settlement manager notified
Lodgement Process completed
Electronic Bank Receipt uploaded to LandCard
Submission of LandCard to negotiating Bank
negotiation of funds by receiving party
transfer of "paid" message to Clearing House
request for payment to drawing Bank
Transfer of funds from drawing Bank to negotiating Bank

Figure 12

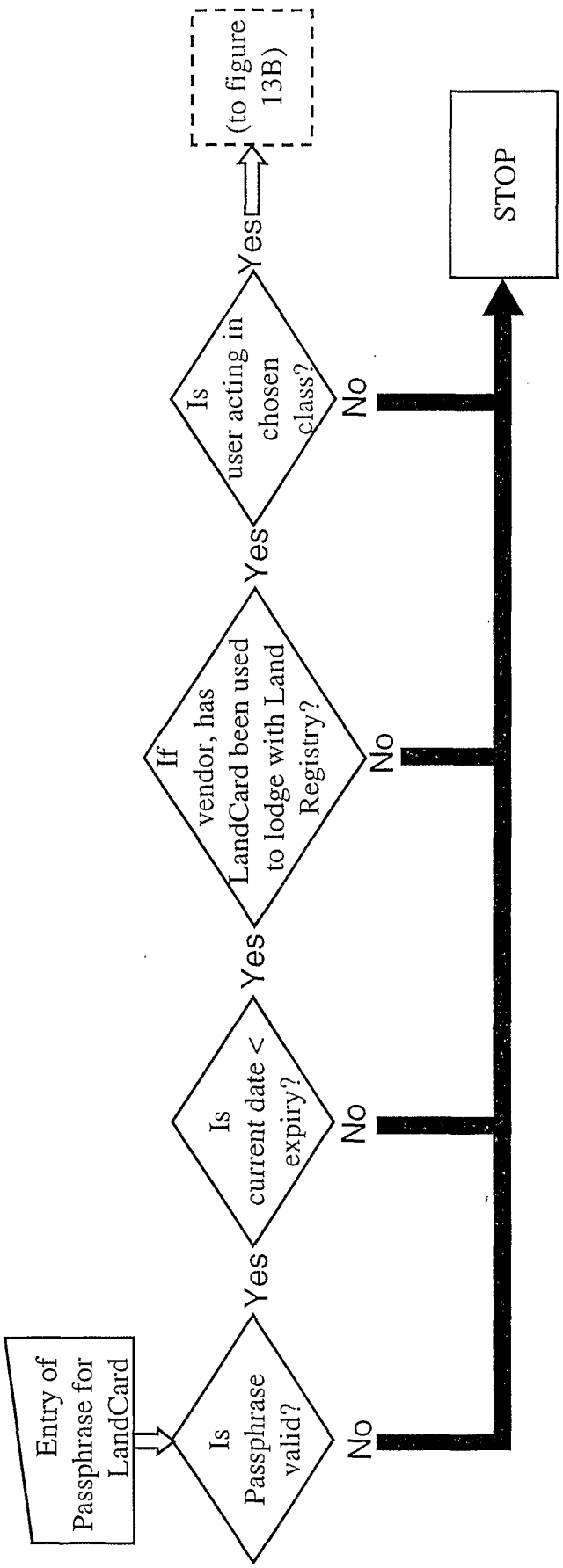

Entry of Passphrase for LandCard
Is Passphrase valid?
Yes
No
Is current date < expiry?
Yes
No
If vendor, has LandCard been used to lodge with Land Registry?
Yes
No
Is user acting in chosen class?
Yes
No
(to figure 13B)
STOP

Figure 13A

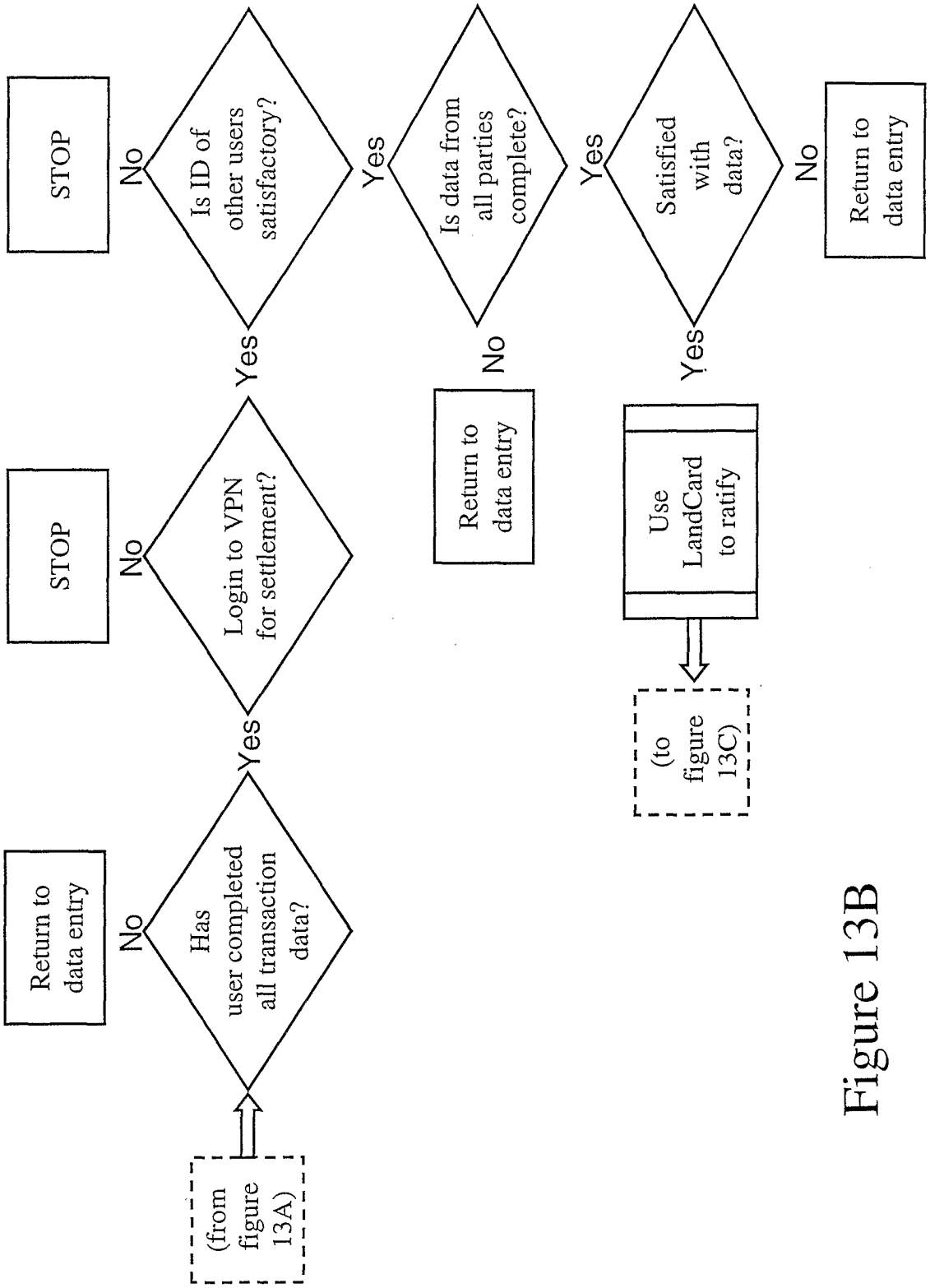

(from figure 13A)
Has user completed all transaction data?
No
Return to data entry
Yes
Login to VPN for settlement?
No
STOP
Yes
Is ID of other users satisfactory?
No
STOP
Yes
Is data from all parties complete?
No
Return to data entry
Yes
Satisfied with data?
No
Return to data entry
Yes
Use LandCard to ratify
(to figure 13C)

Figure 13B

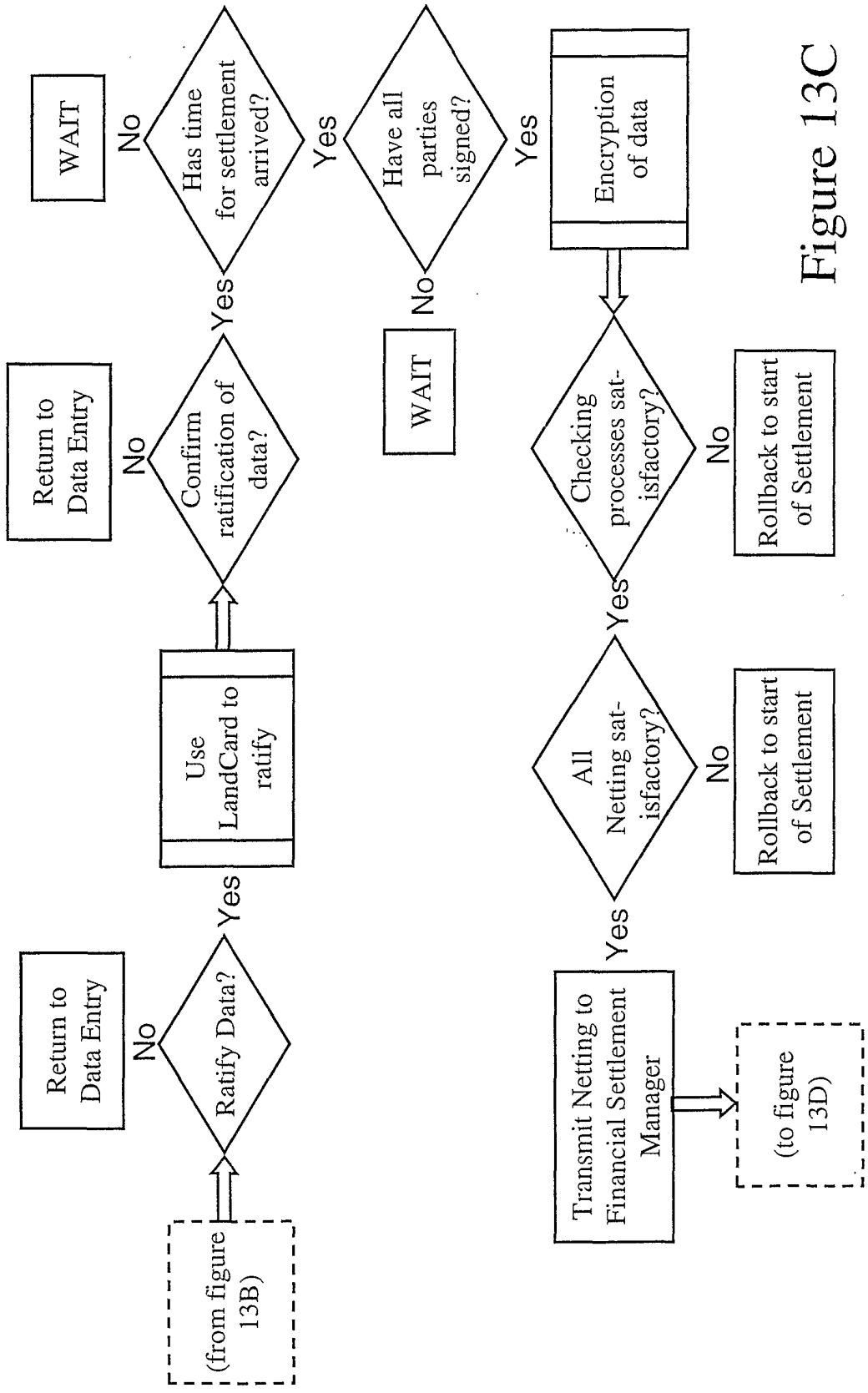

(from figure 13B)
Ratify Data?
No
Return to Data Entry
Yes
Use LandCard to ratify
Confirm ratification of data?
No
Return to Data Entry
Yes
Has time for settlement arrived?
No
WAIT
Yes
Have all parties signed?
No
WAIT
Yes
Encryption of data
Checking processes satisfactory?
No
Rollback to start of Settlement
Yes
All Netting satisfactory?
No
Rollback to start of Settlement
Yes
Transmit Netting to Financial Settlement Manager
(to figure 13D)

Figure 13C

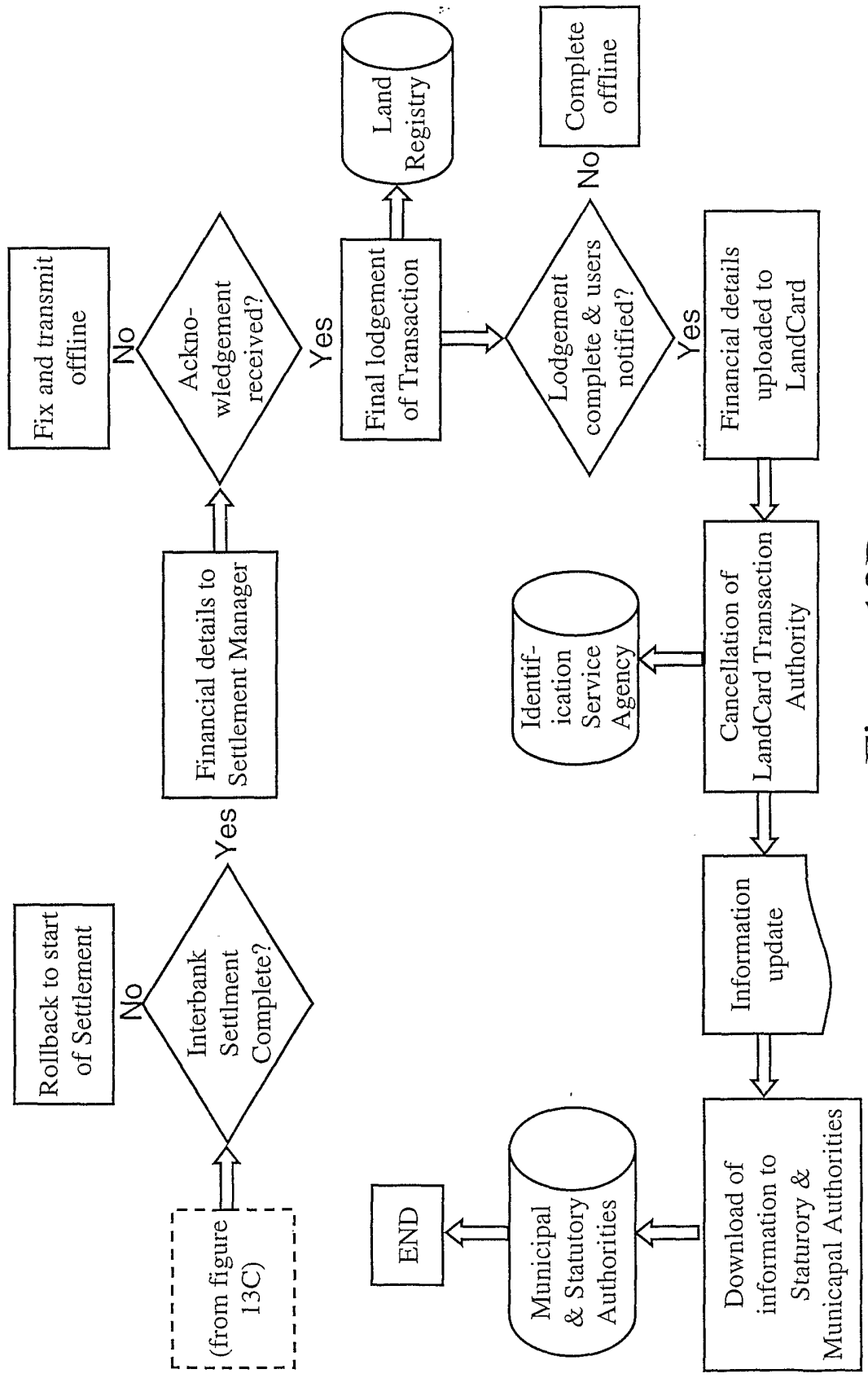

(from figure 13C)
Interbank Settlment Complete?
No
Yes
Rollback to start of Settlement
Financial details to Settlement Manager
Ackno-wledgement received?
No
Yes
Fix and transmit offline
Final lodgement of Transaction
Land Registry
Lodgement complete & users notified?
No
Yes
Complete offline
Financial details uploaded to LandCard
Cancellation of LandCard Transaction Authority
Identif-ication Service Agency
Information update
Download of information to Staturory & Municapal Authorities
Municipal & Statutory Authorities
END

Figure 13D

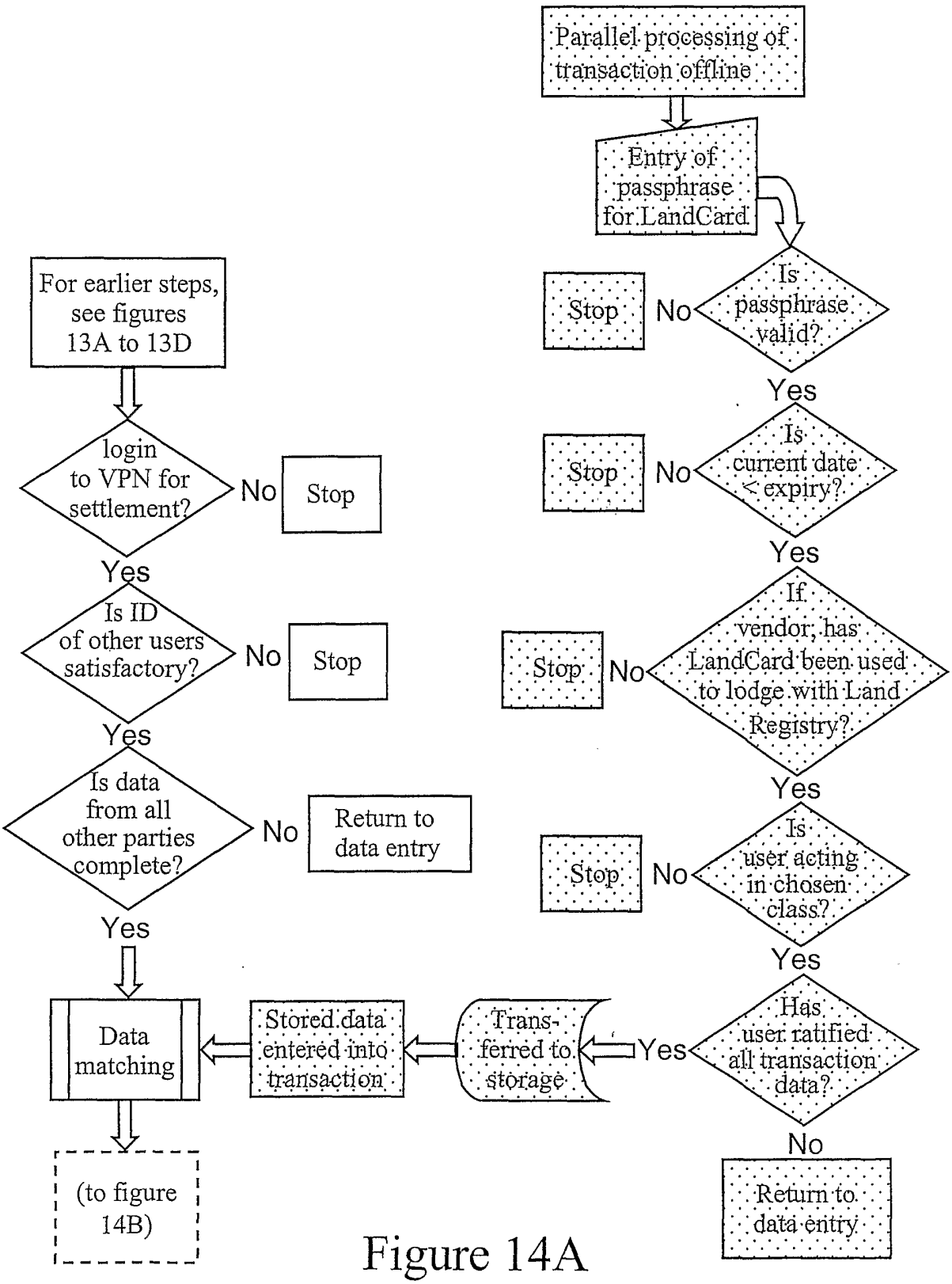

Parallel processing of transaction offline
Entry of passphrase for LandCard
Is passphrase valid?
No
Stop
Yes
Is current date < expiry?
No
Stop
Yes
If vendor has LandCard been used to lodge with Land Registry?
No
Stop
Yes
Is user acting in chosen class?
No
Stop
Yes
Has user ratified all transaction data?
No
Return to data entry
Yes
Trans-ferred to storage
Stored data entered into transaction
Data matching
(to figure 14B)
For earlier steps, see figures 13A to 13D
login to VPN for settlement?
No
Stop
Yes
Is ID of other users satisfactory?
No
Stop
Yes
Is data from all other parties complete?
No
Return to data entry
Yes

Figure 14A

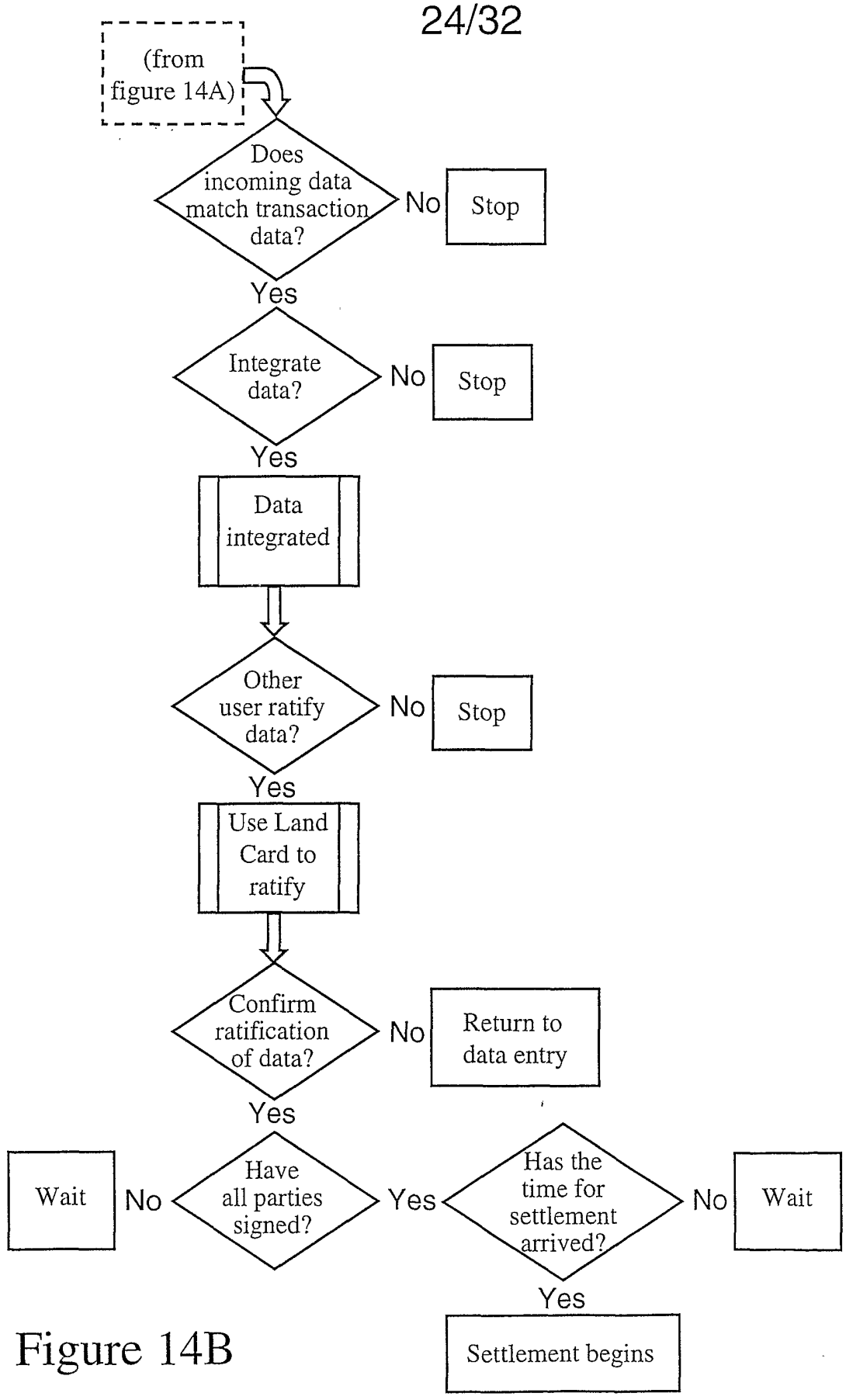
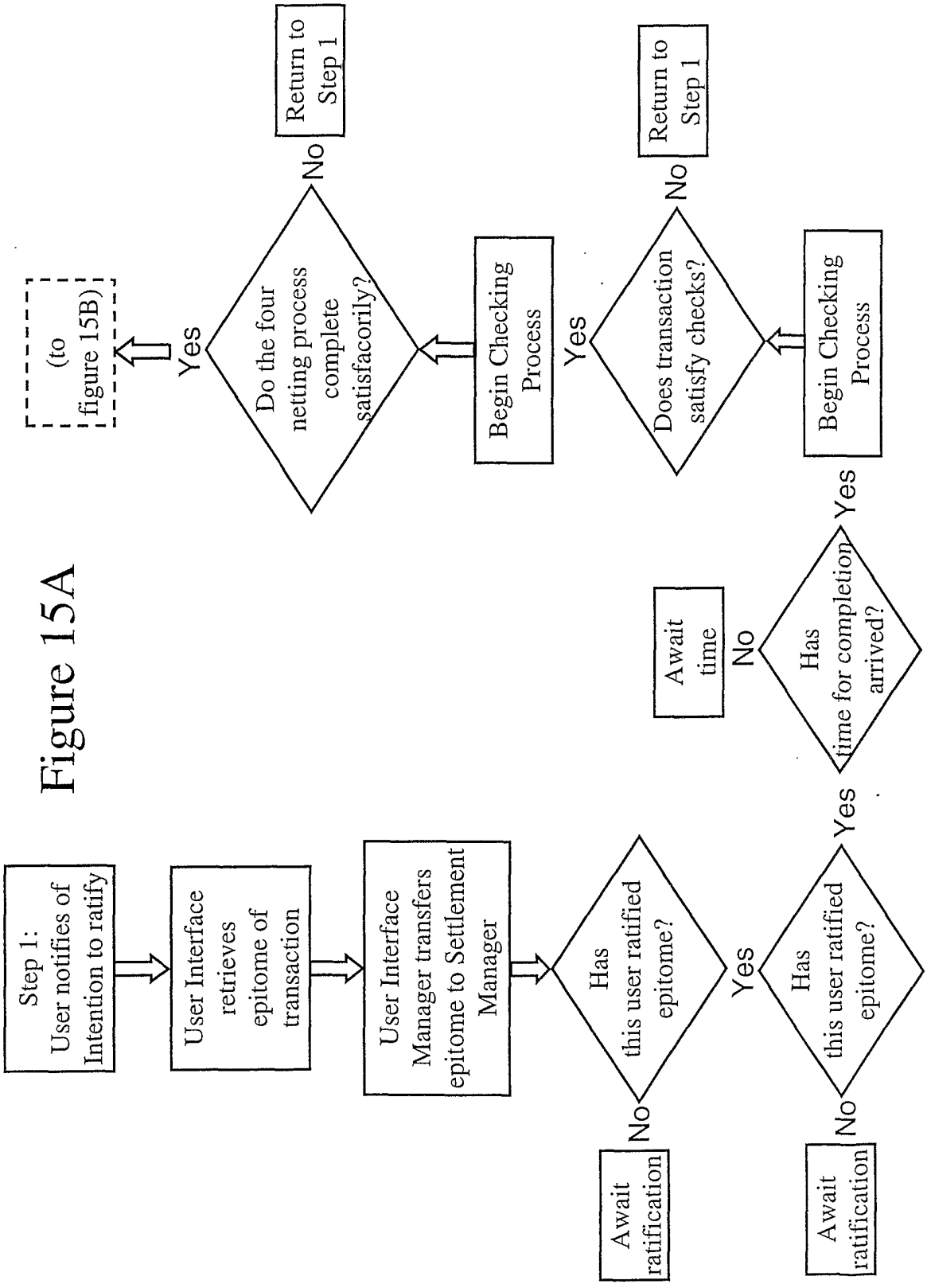

(from figure 14A)
Does incoming data match transaction data?
No
Stop
Yes
Integrate data?
No
Stop
Yes
Data integrated
Other user ratify data?
No
Stop
Yes
Use Land Card to ratify
Confirm ratification of data?
No
Return to data entry
Yes
Wait
No
Have all parties signed?
Yes
Has the time for settlement arrived?
No
Wait
Yes
Settlement begins

Figure 14B

Figure 15A


Step 1: User notifies of Intention to ratify
User Interface retrieves epitome of transaction
User Interface Manager transfers epitome to Settlement Manager
Has this user ratified epitome?
No
Await ratification
Yes
Has this user ratified epitome?
No
Await ratification
Yes
Has time for completion arrived?
No
Await time
Yes
Does transaction satisfy checks?
No
Return to Step 1
Yes
Begin Checking Process
Do the four netting process complete satisfacorily?
No
Return to Step 1
Yes
Begin Checking Process
(to figure 15B)

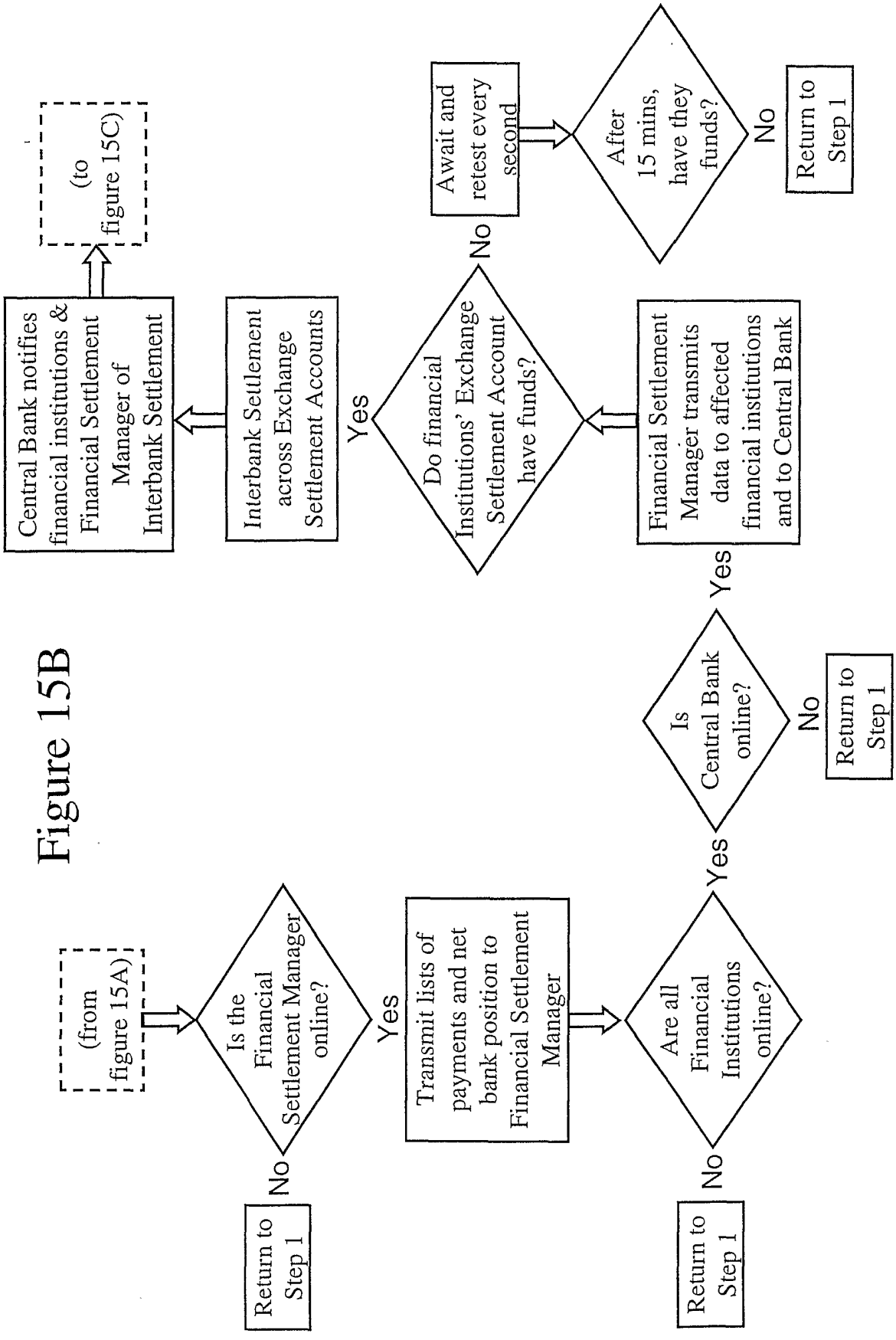
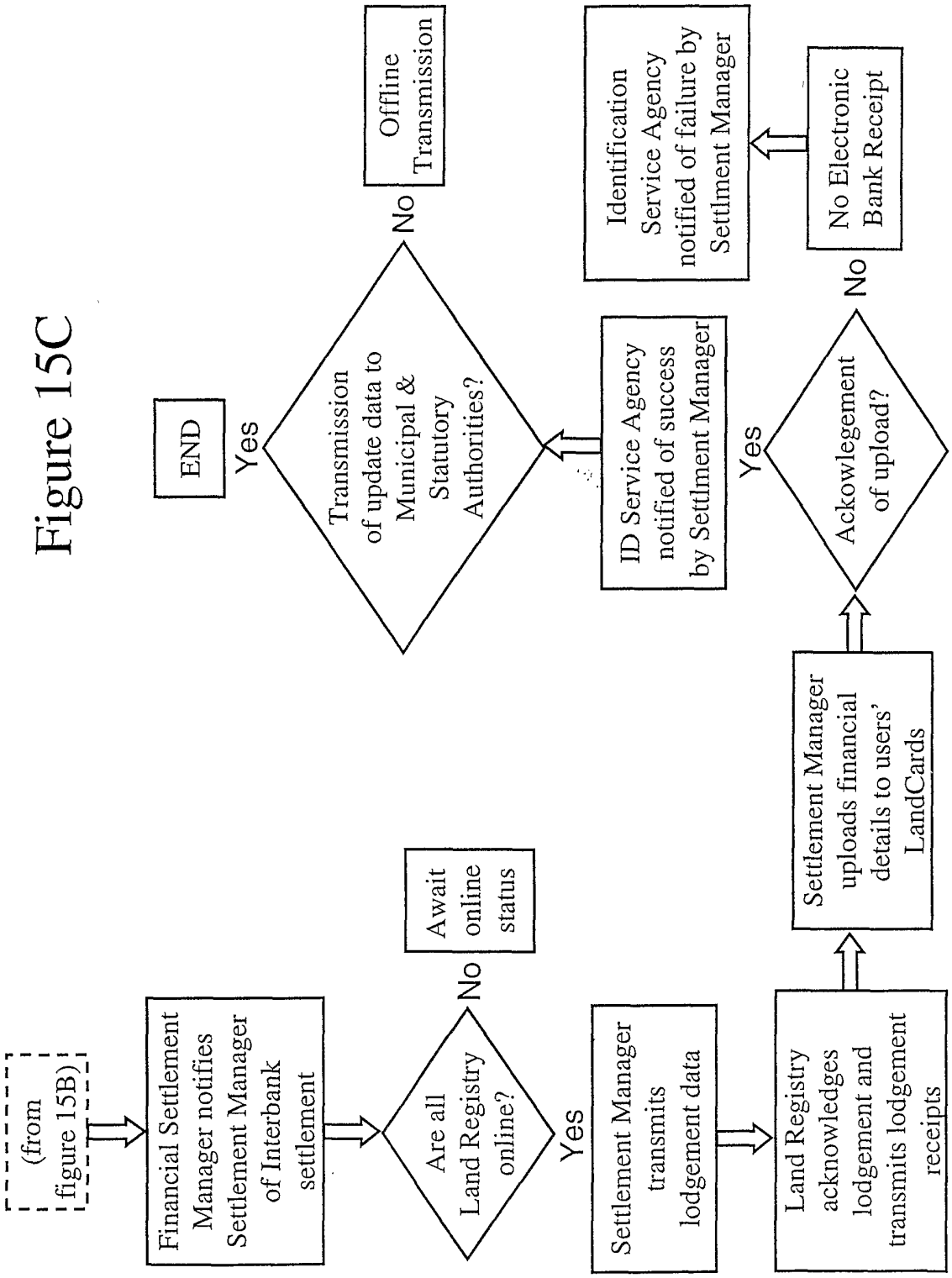

(from figure 15A)
Is the Financial Settlement Manager online?
No
Return to Step 1
Yes
Transmit lists of payments and net bank position to Financial Settlement Manager
Are all Financial Institutions online?
No
Return to Step 1
Yes
Is Central Bank online?
No
Return to Step 1
Yes
Financial Settlement Manager transmits data to affected financial institutions and to Central Bank
Do financial Institutions' Exchange Settlement Account have funds?
No
Await and retest every second
After 15 mins, have they funds?
No
Return to Step 1
Yes
Interbank Settlement across Exchange Settlement Accounts
Central Bank notifies financial institutions & Financial Settlement Manager of Interbank Settlement
(to figure 15C)

Figure 15B

Figure 15C


(from figure 15B)
Financial Settlement Manager notifies Settlement Manager of Interbank settlement
Are all Land Registry online?
No
Await online status
Yes
Settlement Manager transmits lodgement data
Land Registry acknowledges lodgement and transmits lodgement receipts
Settlement Manager uploads financial details to users' LandCards
Ackowlegement of upload?
No
No Electronic Bank Receipt
Identification Service Agency notified of failure by Settlment Manager
Yes
ID Service Agency notified of success by Settlment Manager
Transmission of update data to Municipal & Statutory Authorities?
No
Offline Transmission
Yes
END

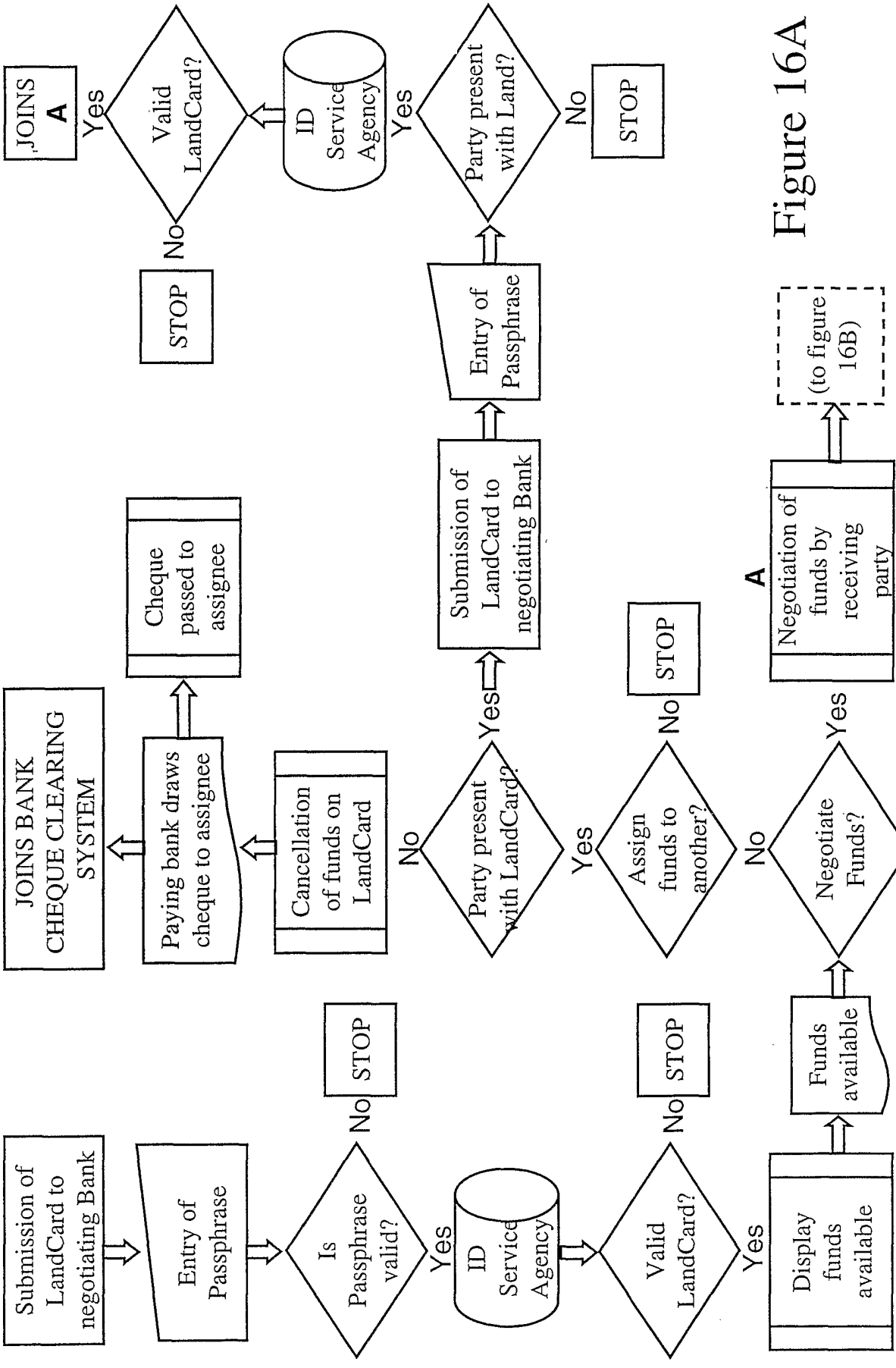
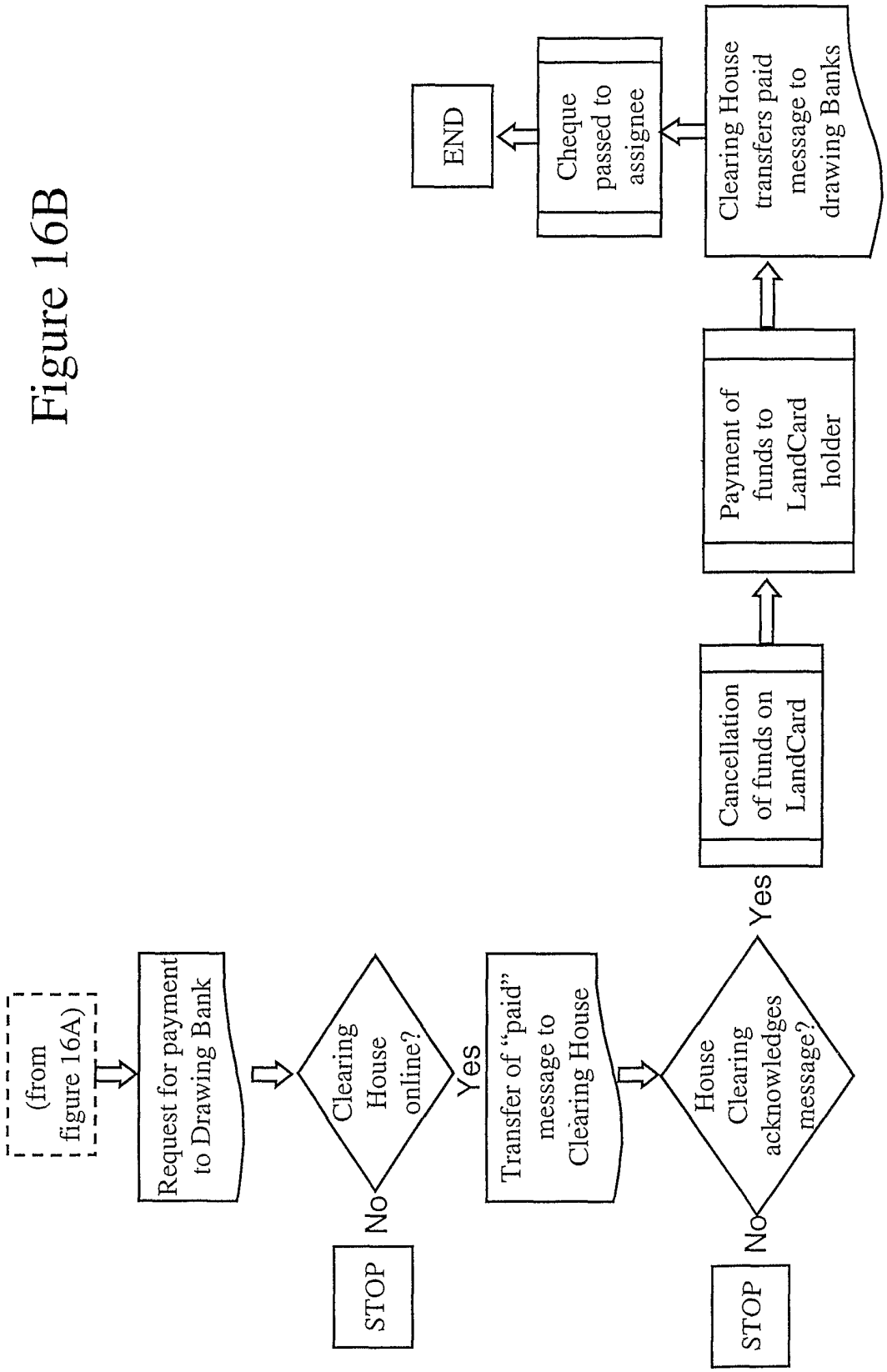

Submission of LandCard to negotiating Bank
Entry of Passphrase
Is Passphrase valid?
No
STOP
Yes
ID Service Agency
Valid LandCard?
No
STOP
Yes
Display funds available
Funds available
Negotiate Funds?
No
Assign funds to another?
No
STOP
Yes
Party present with LandCard?
No
Cancellation of funds on LandCard
Yes
Paying bank draws cheque to assignee
JOINS BANK CHEQUE CLEARING SYSTEM
Cheque passed to assignee
Submission of LandCard to negotiating Bank
Entry of Passphrase
Party present with Land?
No
STOP
Yes
ID Service Agency
Valid LandCard?
No
STOP
Yes
JOINS A
A
Negotiation of funds by receiving party
(to figure 16B)

Figure 16A

Figure 16B


(from figure 16A)
Request for payment to Drawing Bank
Clearing House online?
No
STOP
Yes
Transfer of "paid" message to Clearing House
House Clearing acknowledges message?
No
STOP
Yes
Cancellation of funds on LandCard
Payment of funds to LandCard holder
Clearing House transfers paid message to drawing Banks
Cheque passed to assignee
END

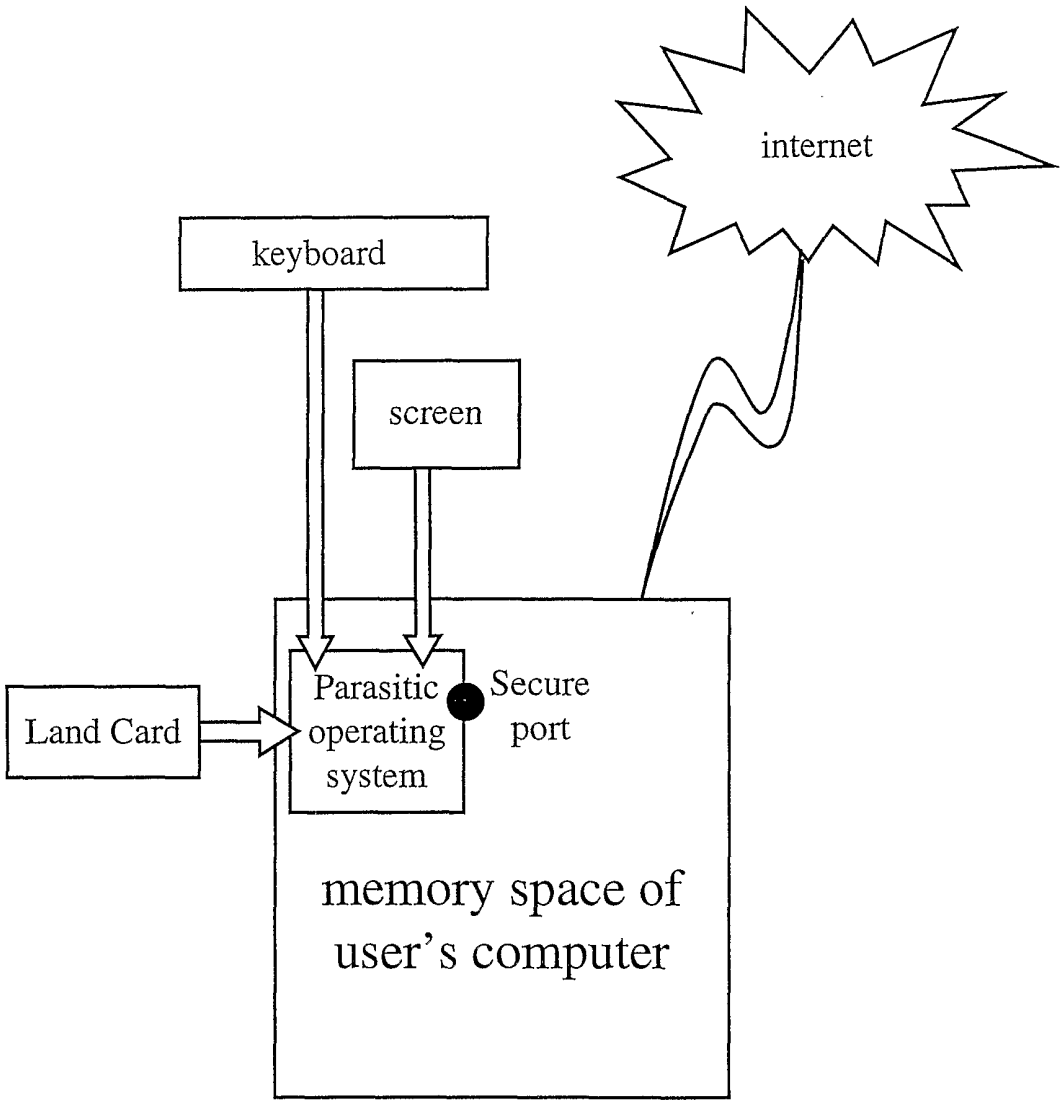

internet
keyboard
screen
Land Card
Parasitic operating system
Secure port
memory space of user's computer

Figure 17

Figure 18

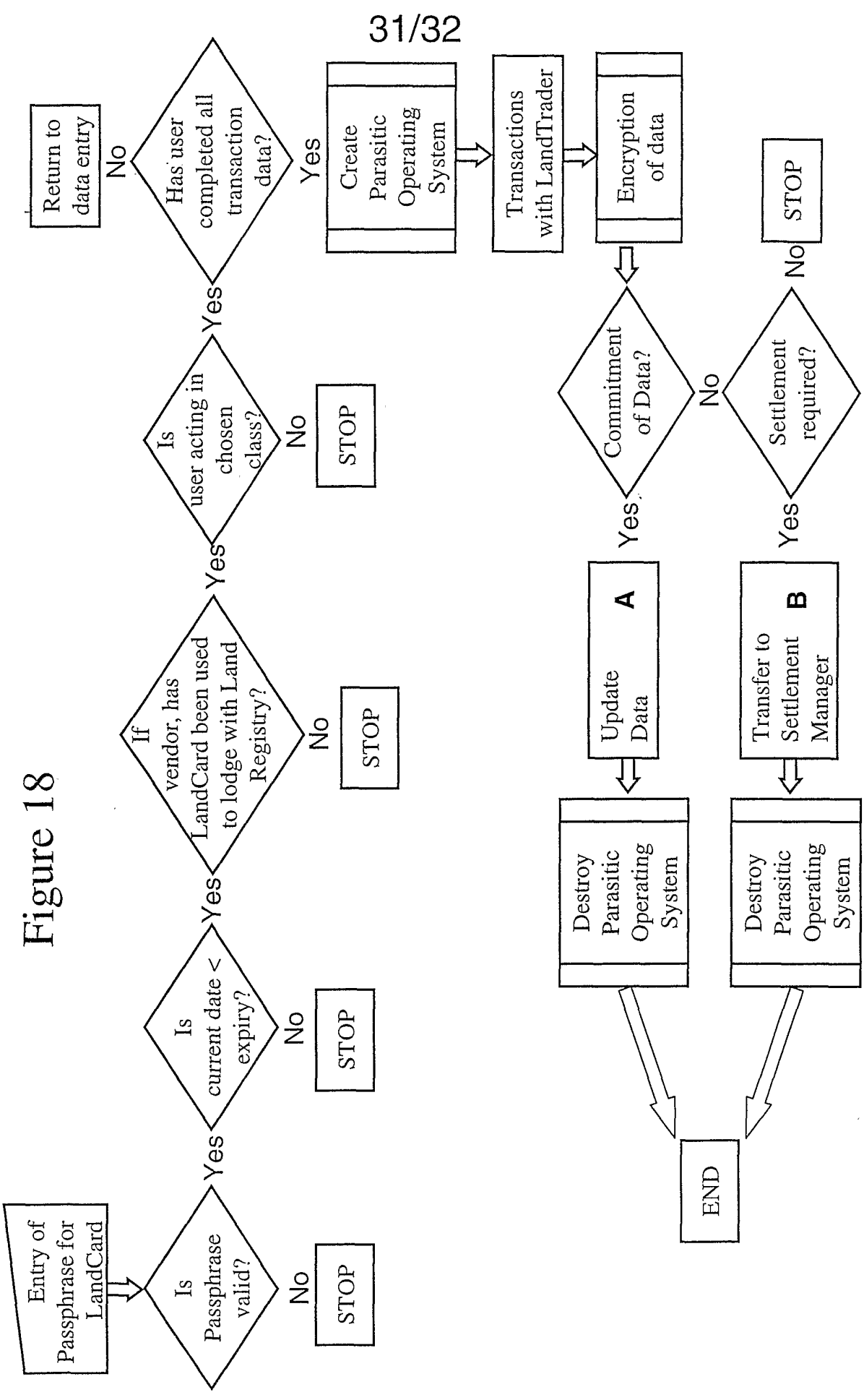
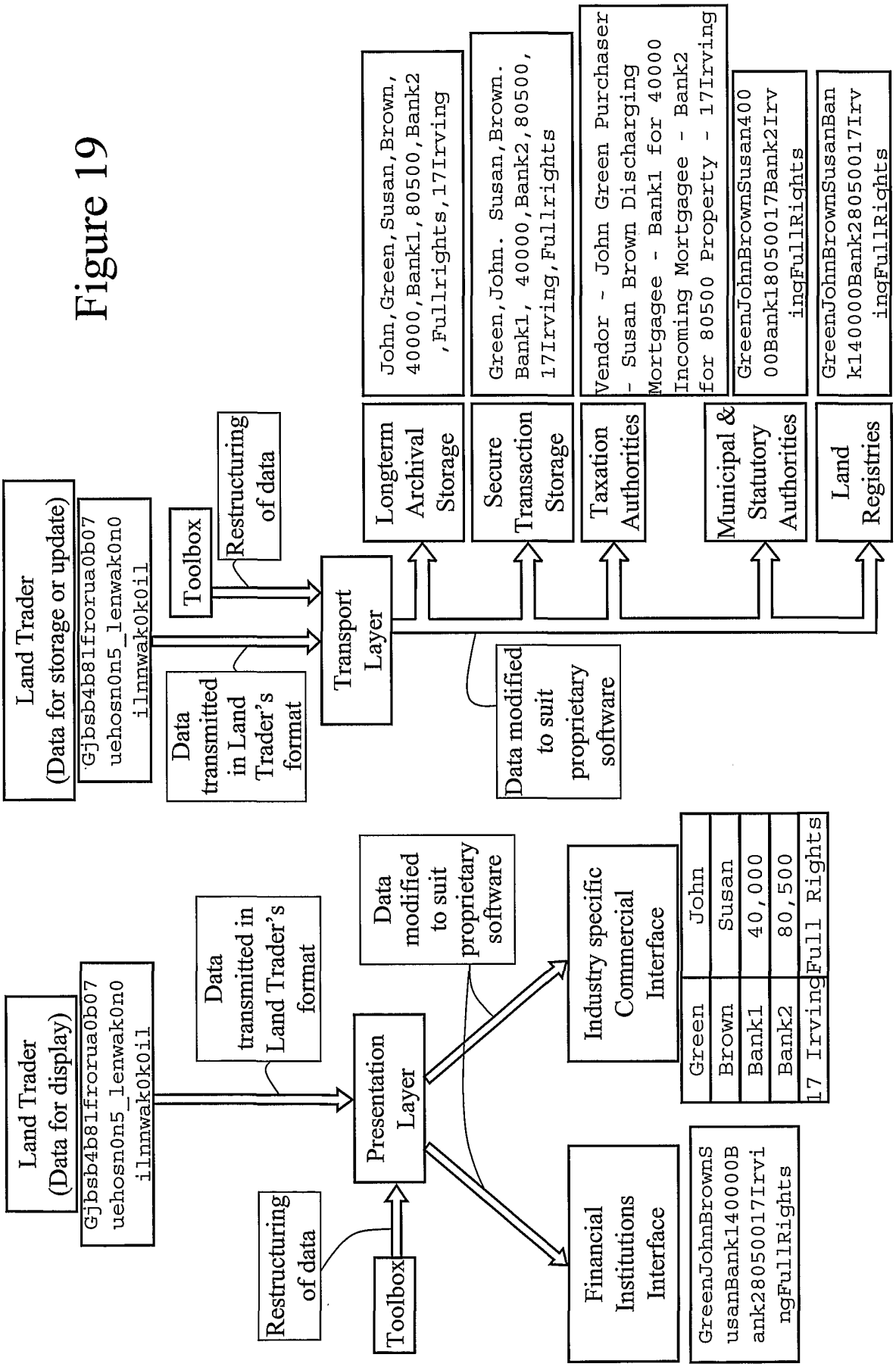

Entry of Passphrase for LandCard
Is Passphrase valid?
No
STOP
Yes
Is current date < expiry?
No
STOP
Yes
If vendor, has LandCard been used to lodge with Land Registry?
No
STOP
Yes
Is user acting in chosen class?
No
STOP
Yes
Has user completed all transaction data?
No
Return to data entry
Yes
Create Parasitic Operating System
Transactions with LandTrader
Encryption of data
Commitment of Data?
Yes
Update Data
A
Destroy Parasitic Operating System
No
Settlement required?
Yes
Transfer to Settlement Manager
B
Destroy Parasitic Operating System
No
STOP
END

Figure 19


Land Trader (Data for storage or update)
Gjbsb4b81frorua0b07 uehosn0n5_lenwak0n0 ilnnwak0k0il
Toolbox
Restructuring of data
Data transmitted in Land Trader's format
Transport Layer
Data modified to suit proprietary software
Longterm Archival Storage
Secure Transaction Storage
Taxation Authorities
Municipal & Statutory Authorities
Land Registries
John,Green,Susan,Brown, 40000,Bank1,80500,Bank2 ,Fullrights,17Irving
Green,John. Susan,Brown. Bank1, 40000,Bank2,80500, 17Irving,Fullrights
Vendor - John Green Purchaser - Susan Brown Discharging Mortgagee - Bank1 for 40000 Incoming Mortgagee - Bank2 for 80500 Property - 17Irving
GreenJohnBrownSusan400 00Bank18050017Bank2Irv ingFullRights
GreenJohnBrownSusanBan k140000Bank28050017Irv ingFullRights
Land Trader (Data for display)
Gjbsb4b81frorua0b07 uehosn0n5_lenwak0n0 ilnnwak0k0il
Data transmitted in Land Trader's format
Presentation Layer
Data modified to suit proprietary software
Industry specific Commercial Interface
Green John
Brown Susan
Bank1 40,000
Bank2 80,500
17 Irving Full Rights
Restructuring of data
Toolbox
Financial Institutions Interface
GreenJohnBrownSusanBank140000Bank28050017IrvingFullRights

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU02/00317

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06F 17/60, G06K 19/07

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)

G06K 19/07

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, DWPI (smart cart, transaction, visa, operating system, instrument)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00/62220 A (ILUMIN CORPORATION) 19th October 2000 the whole document	1-13, 20-34
X	US 4,812,628 A (BOSTON et al) 14th March 1989 the whole document	1-13, 20-34
X	US 5,649,118 A (CARLISLE et al) 15th July 1997 the whole document	1-13, 20-34

[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
11 June 2002	21 JUN 2002
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	**J. W. Thomson** Telephone No : (02) 6283 2214

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU02/00317

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,721,781 A (DEO et al) 24th February 1998 the whole document	1-13, 20-34
X	US 6,101,477 A (HOHLE et al) 8th August 2000 the whole document	1-13, 20-34
X	US 4,766,293 A (BOSTON) 23rd August 1988 the whole document	1-13, 20-34
X	US 6,005,942 A (CHAN et al) 21st December 1999 the whole document	1-13, 20-34
X	US 5,844,218 A (KAWAN et al) 1st December 1998 the whole document	1-13, 20-34
X	US 6,170,742 B (YACOOB) 9th January 2001 the whole document	1-13, 20-34
A	US 6,167,378 A (WEBBER, JR.) 26th December 2000 the whole document	1-36

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU02/00317

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					
WO	200062220	AU	200040787	AU	200044606	EP	1171811
		EP	1177517	WO	200062143		
US	4812628	AU	56546/86	CA	1252566	EP	200343
		US	4734564				
US	5649118	BR	9403345	CA	2117440	EP	640945
		JP	7182426				
US	5721781	NONE					
US	6101477	AU	23362/99	EP	1050027	GB	2333630
		GB	2351379	WO	9938129		
US	4766293	AU	72559/87	CA	1270326	EP	251619
		JP	63257089				
US	6005942	AU	65786/98	EP	1004992	EP	1021801
		US	6233683	WO	9843212		
US	5844218	AU	14282/97	EP	912953	WO	9802834
		ZA	9610705				
US	6170742	WO	9748040				
US	6167378	AU	60307/98	WO	9834167		

END OF ANNEX