In JHP Eloff (ed), Proceedings of the IFIP TC11 Workgroup 11.2 on Small System Security, Samos, Greece, May 1996

A Prototype for Personal Business Transactions on Public Networks

Eric J Uphof and Martin S Olivier
Rand Afrikaans University*

Abstract

This paper describes a prototype system that illustrates the use of a public network (such as the Internet) for personal financial and business transactions. It is assumed that the public network cannot be trusted and that the prototype system has to ensure secrecy, non-repudiation and other guarantees required for acceptance of such a system. In addition it is assumed that the user is not necessarily a technical expert—all technical aspects (including that associated with encryption) therefore has to be hidden from the user.

The system is structured as a sales interface, that forms the control centre of the system, a registration package which the user initially uses to register on the system, an ordering platform through which orders are placed, an advertisement placement platform used to advertise goods on the system, a bank manager that forms the interface with a virtual bank and an advertisement viewing component that may be used by registered and nonregistered users.

1 Introduction

Current trends show that there is an increased interest in the Internet as a source for information not only for the business orientated users but also private users. In fact, the recent past has seen a scramble by financial institutions and industry to establish a presence on *The Net* [2]. *"Long viewed as a refuge for academics, researchers, and hackers, the Internet has taken a significant step towards becoming a national electronic marketplace with a new high-speed business-to-business network called CommerceNet ... [which] permits Internet-connected companies and individuals to buy and sell goods..."* [3].

*Address correspondence to Department of Computer Science, Rand Afrikaans University, PO Box 524, Auckland Park, Johannesburg, 2006 South Africa; E-mail: molivier@rkw.rau.ac.za

These trends are due partly to the ease to which one can be connected to the Internet. Mechanisms are already available that enables a client to communicate securely with a server on the Internet [4]. This paper describes a system that only allows users registered with the system to engage in commercial transactions. Nonregistered users are allowed to view advertisements to entice them to register with the system.

The system differs from similar systems in primarily two ways: Firstly the system is not maintained by the seller of the goods, but by an independent third party who charges a fee for this service, and provides certain guarantees for both buyers and sellers. Secondly, the system operates asynchronously—users, for example, do not have to wait online for payment to be authorised. From a security point of view it is also important to note that a user is requested to verify a transaction before it is finalised—because of the asynchronous nature of the system this makes it more difficult to fabricate a message.

2 Background

This paper focusses on the security side of a system that enables trading on a public network. As such it has to address the usual three primary issues: confidentiality, integrity and availability. Since the system handles financial and personal information, it must be ensured that such information is not accessible to unauthorised users. On the integrity side it is important to ensure that transactions (and other information) is not tampered with by unauthorised users. And a system which is not available will not be entrusted money and goods for sale by users.

A requirement of any such system is that of non-repudiation: the ability of a receiver to prove that a received message was indeed sent by a purported sender. Otherwise a buyer may afterwards claim that the message to buy was never sent and the delivered goods not wanted.

For most of the requirements listed above, encryption forms the most important solution in the given circumstances. Encryption algorithms are either symmetrical or use a public/secret key combination. A symmetric algorithm uses the same key for encryption and decryption. A public key system uses one key for encryption and another for decryption. In such systems the one key is made public, while the other key is kept secret. The secret key cannot be derived from the public key. We will assume that any of the two keys can be used to encrypt a message, which can then be decrypted with the other key. The RSA algorithm is the best-known example of a public key encryption system, and will be used in this paper. The RSA algorithm allows either the public or the secret key to be used as encryption key; the other key can then be used as decryption key.

Public key algorithms can also be used to electronically sign a message. In

the simplest form a message encrypted with a user's secret key proves that the message was sent by that user: Since the public key of a user is commonly known and since the public key can only decrypt a message encrypted with the corresponding secret key it proves that that particular secret key was used. And since that secret key is only known to the concerned user it proves that such a message was indeed sent by the user.

See [1] for more information on encryption in general, as well as the RSA algorithm and its use for electronic signatures.

It is widely accepted that the World Wide Web will be the platform on which most initial commercial systems on the Internet is based. Secure versions of the protocols used on the Web have already been implemented: amongst others SSL (secure sockets layer) and SHTTP (secure hypertext transfer protocol) can be used to ensure confidential (and even signed) communication, while STT (secure transaction technology) and SEPP (secure electronic payment protocol) provide the possibility for a site to engage in transactions with and unknown party [4]. The prototype described in this paper is not intended to form an alternative for any of these protocols; in fact its operation corresponds to these protocols in the important respects. The prototype is rather intended to illustrate one particular architecture to structure a 'shopping mall' that enables buyers and sellers to get together and to interact.

The prototype described in this paper requires a confirmation by the user before a transaction is completed. This confirmation will follow a random time after the transaction has been initiated, making it unlikely that a transaction can be initiated by a person who walks past an unattended workstation on behalf of the user logged into that workstation. Since this is not easy on the current version of the Web, the prototype described in this paper is not based on the Web, but on specially developed software. The approach described in this paper can, however, be used on a combination of the Web and electronic mail software once transparent encryption from typical electronic mail packages becomes a reality.

The primary goals of the prototype described in this paper are described next.

2.1 Primary goals of the system

The system must achieve certain goals; these range from security aspects to commercial aspects. Some of the goals identified are

1. Secrecy of all transactions (monetary and other) between the users and the control centre of the system.
2. Non-repudiation and authentication of the users of the system.
3. Audit trails must be kept of all transactions in the system.
4. Interface to various banks using a credit card facility (for monetary transactions).

5. The various user applications must be available on multiple platforms.
6. The advertisements placed by a user should be seen by users across the world via the control centre.
7. Orders placed must follow general transaction rules. Validity of money in account. Validity of number of items ordered.
8. All correspondence is to an e-mail address users must therefore have an e-mail address.
9. All processing at the control centre is autonomous—no human interaction is needed.
10. Billing details and usage details need to be kept for users of the system at the control centre.
11. The system must be fully expandable.
12. All user applications must be simple and easy to use.
13. The control centre must be able to recover from errors and always be available.

3 System architecture

A domain policy is used in the system architecture. Each of these domains is self-supporting and contains a control centre which regulates and controls all users in the domain.

The system developed is composed of a number of modules—these being distributed between the users and a control centre: The *sales interface* (control centre of the system) is responsible for the organisation and management of the system. A *registration package* enables a person to register with the system as a buyer or seller. The *ordering platform* will be distributed to clients who register as buyers. The *advertisement placement platform* will be distributed to clients who register as sellers. The *bank manager* is used to communicate with a virtual bank. This facility can be used to deposit, withdraw money or inquire about a bank balance. The ordering platform, advertisement placement platform and bank manager are combined into a *client package* that provides an integrated interface to the buyer and/or seller. The components of the system are depicted in figure 1.

Other modules which enable users to retrieve advertisements and retrieve short stock lists are also available. All of these user modules communicate with only one sales interface and always with that sales interface. Some public network

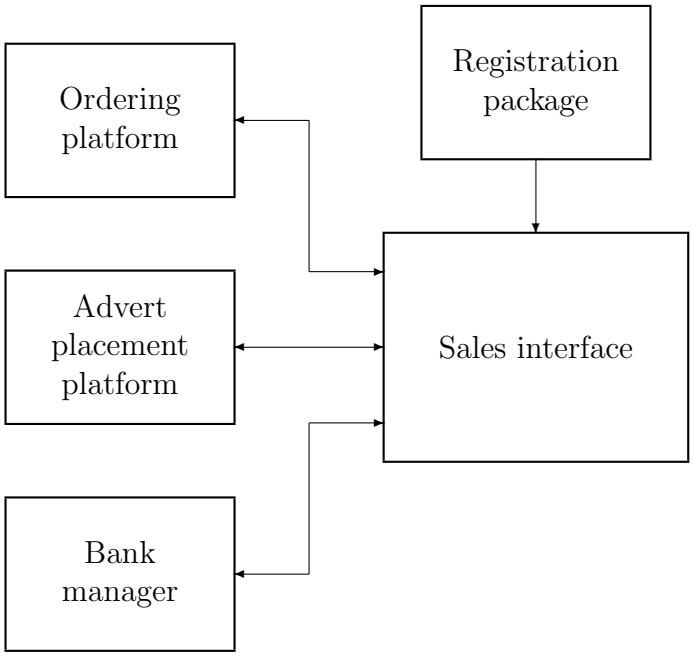

Figure 1: Basic components of architecture

provides the communication medium for the communications between the various parties.

The system as described above is a very basic structure, which can be expanded to meet demands. A sales interface can have a multitude of clients; each client will own either an ordering platform if that client is a buyer or an advertisement placement platform if that client is a seller, or potentially both if the client is both a seller and a buyer. The sales interface and all the client platforms with witch it will communicate form a single domain and will be controlled by the control centre (sales interface) in that domain. We are able to expand the above basic architecture to a more elaborate one by introducing multiple domains, each linked together through the control centre (sales interface) for the domain and using a (public) backbone network to supply the communications medium. This is depicted in figure 2.

The various domains (each of which contains a sales interface which is the control centre for that domain) is self supporting. Inter-domain communication when required is performed by the sales interfaces for the respective domains.

This approach holds a number of benefits. Firstly, it allows for easy expansion without affecting existing modules in the system. The subdivision into domains results in better management of the system as a whole as management of a domain will not affect other domains in the system. A buyer and seller never communicate directly until such point that a transaction between the two has

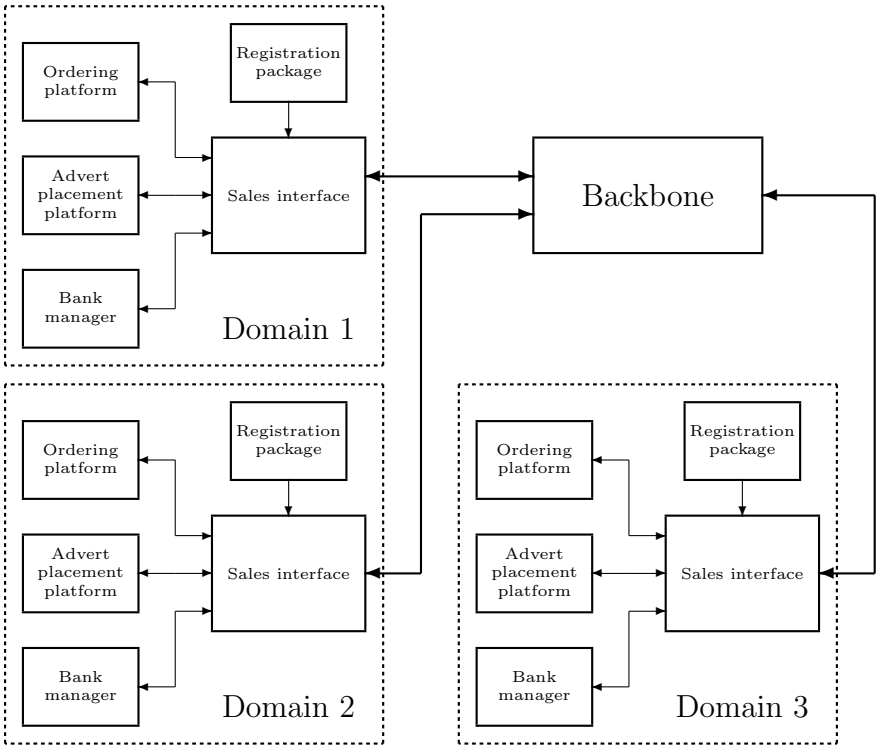

Figure 2: Multiple domains architecture

taken place. This adds to the security of keeping client details private until such time as they need to be exchanged. As all transactions are processed through the system, the system can deduct commissions where applicable. And, finally, the sales interface, being the only access to the system, can do security and authorisation checks.

The described approach also has a number of disadvantages. A bottleneck can potentially form at the sales interface since any access to the sales interface must first be authorised by the security manager of the sales interface. In addition, if the user wishes to change sales interfaces, the client's packages have to be modified such that all future communications would take place between the client and the new sales interface.

4 System components

This section describes each of the components of the sales system in more detail.

4.1 Sales interface

The sales interface is the control centre of the system—all communication must go through the sales interface. The sales interface components include

1. The *security module* restricts access to authorised users.
2. The *transactions manager* controls all transaction processing.
3. The *storage facility* is subdivided into secure storage and non-secure storage.

   Secure storage is encrypted and includes bank details, security details, personal Details, stock details, logs (for audit purposes) and transactions pending (that is, transactions started but not yet completed).

   Non-secure storage is not encrypted and includes advertisements of stock and the stock list of items available.
4. The *directory* contains all addresses for sales interfaces in other domains for inter-domain communications.
5. The external communication link to a bank using a speed point type access for credit card transactions.

The sales interface has a number of duties to perform. This includes the registration of new clients and generation of security keys for new clients. Note that, since the sales interface generates secret keys on behalf of users, a message encrypted with the client's key proves to the sales interface that the message originated from the client. However, it does not prove to a third party that the sales interface did not fabricate the message. Users therefore have to trust the sales interface. The sales interface is also responsible for the distribution of packages to clients enabling them to perform transactions, performing client transactions, controlling logical bank accounts for clients and debiting and crediting of physical bank account through credit card technology. The sales interface also handles inter-domain transactions on behalf of a client. Finally, the sales interface controls the advertisement board (including the update, deletion and creation of advertisements).

4.2 Registration package

The registration package enables a person to register as a client to the system. A client can either be a buyer, a seller, or both buyer and seller. The registration package must be available for various operating system platforms. The package asks for information from the potential client. A vital part of this package is the initial input of a PIN (personal identification number) which is user defined. This PIN will have to be entered each time the client wishes to initiate a transaction.

Another vital input is that of an electronic address to which all transactions are sent for that client. This address must be a valid address which refers to the client uniquely. Other important details are those of the bank name and bank account. This data refers to an external bank on which monetary withdrawals and monetary deposits can be made. All this information together with other personal information is encrypted using a RSA encryption key which can only be decrypted by the sales interface. This ensures privacy of data. Once the registration package has been used it may be discarded as it will never be required again.

The following steps are followed to register as a client:

1. The new client has to find the sales interface for the appropriate domain. (This sales interface will generally be the closest one to the new client. Being the closest sales interface the cost of communication is kept to a minimum.)

2. The new client now uses FTP to download the registration executable file for the respective operating system to be used. There could potentially be a different registration file for every different operating system.

3. Execute the registration file and fill in all details as asked for. In particular, an electronic address where the sales interface may contact the client has to be supplied. Additionally the client has to specify bank account details (of a physical bank account), the type of client he/she wishes to be (buyer and/or seller) and a PIN which must be given for all future communications between the client and the sales interface.

4. The sales interface will verify these details and send the client interface applications which must be used for all future communications with the sales interface.

It is the responsibility of the sales interface to read all the details of the new client, to verify the bank details against the respective bank organisation and to generate packages specific to the client. The PIN is stored and used for future client authentication. The packages generated for the client are the only packages which the client can use to interact with the sales interface. The packages generated include RSA encryption keys that will be used in all future communications between the client and the sales interface. Should there be at any stage a breach in the security of the communications between the sales interface and the client, the sales interface would need to regenerate the packages with new RSA cryptographic keys.

4.3 Ordering platform

Before having access to the ordering platform the client must be registered as a buyer in the system. At registration the client will be presented with the appropriate packages. Having the ordering platform allows the client to place an order for an article which he can see in an advertisement. This package is unique to that client in that each package contains a unique key used to encrypt all further communications between it and the sales interface. This package also has hard-coded into it the address of the sales interface with which it will communicate. Using this method the client need never store a sales interface address and the message will always go to the same sales interface. For a transactions to be successful, the client will need to submit the transaction from his own ordering platform and will be required to give the PIN which the client specified at registration time. The transaction created will be sent to the sales interface at which point it will be checked for authenticity. In this approach the respective sales interface will be aware of all attempts (legal or illegal) to access the system. It can keep track of potential hackers and notify the client of illegal attempts from his ordering platform. The Security of the communication between the sales interface and the ordering platform is achieved using the RSA encryption algorithm which provided the fundamental integrity of the data in the transaction and the non-repudiation required for monetary transactions.

The following steps are followed to order an article:

1. Locate the advertisement number of the advertisement for which you wish to place an order for.

2. Ensure you have enough money in your account to place the order. If there are insufficient funds you will not be allowed to place the order.

3. To place the order run the ordering platform and complete the necessary details. Specify the control centre where that advertisement is placed. This facility does not restrict you to buy from only the control centre that you are registered with, but from any control centre in any domain as long as the item is available.

4. The transaction is then sent to the sales interface where it is processed. Should there be insufficient funds the order will not be allowed. Should the quantity ordered not be available, you will be given the option to order the remaining amount.

5. After the initial ordering of the items you will need to confirm any order. You have the option to confirm at which point the order will be placed and you will be notified of the seller of that product. Likewise the seller will be notified of who bought the product and the number of items bought.

6. This information can now be used to arrange delivery of the products.

All order transactions are logged for audit purposes. These audit files may serve as proof of purchase should there be any discrepancy between the buyer and the seller.

Once the initial step of the order is completed and the sales interface waits for the confirmation from the client, the articles which the client has ordered are locked and cannot be sold to anyone else. Where you are ordering from a control centre not in your own domain, your order is still placed at your own control centre. The control centre will communicate with the relevant control centre in an attempt to place the order. It should be noted that there is no preference given to any domain or client in a domain. All orders are placed on first come first served basis.

4.4 Advertisement placement platform

Only clients registered as sellers may place advertisements so as to sell their products. At registration time such a client will be presented with a package that will enable the client to send advertisements to the sales interface. This package is once again unique to the client and must be used by that client in order to have the advertisement successfully placed. The package, as with the ordering platform, contains an RSA key which is used in conjunction with the user's PIN (specified at registration time) to encrypt all messages between the client and the sales interface. This provides the non-repudiation and confidentiality of the transaction.

Once the client has placed an advertisement this client has no further control over it. The control centre will adjust stock counts and control bank balances when the stock is sold. The client will be notified of who has bought the stock and the quantity bought so that arrangement for delivery can be made.

The following steps will place an advertisement:

1. Construct a visually appealing advertisement for your article and save as a file (File types may be any one of the following WINDOWS BMP ; GIF Format ; MPEG Format ; WINDOWS AVI ; Text Based).

2. Execute the advertisement placement platform and fill in all the details for the articles you wish to advertise, including the number of items and the price for a single item.

3. At the control centre your advertisement will be temporarily placed but will not be appended to any stock lists until you confirm the advertisement placement.

4. On confirmation of the advertisement placement (which is only possible by the client placing the advertisement) the advertisement will be placed on the short list and will be accessible for an advertisement query.

Stock numbers will be controlled by the control centre and the seller client will be notified when a buyer client has purchased a quantity of stock. As soon as the quantity available for a particular item of stock reaches zero the stock is automatically removed from the stock list and no more of those items can be ordered.

4.5 Bank manager

A client who is registered has a logical or virtual bank account with the control centre which handles that client's requests. The account is created at registration time with an initial balance of zero. All monetary transactions affect this bank balance. When wishing to place an order a client must ensure that there is money available in this bank account.

At registration time all clients are presented with a bank manager which enabled the client to control his bank account. Operations which can be performed include requesting the bank balance, depositing money into the bank account and withdrawing money from the bank account.

To request a bank balance the client has to execute the bank manager and select the option 'request bank balance', after which the control centre will process the request and notify the client of the bank balance.

Similarly, to deposit money into the bank account the client will execute the bank manger and select the option for depositing money and enter the amount to be deposited. The control centre will process the request and attempt to withdraw the amount specified from the client's external bank (which the client specified at registration time). If the deposit is allowed, the client will need to confirm the deposit. Likewise if the deposit is not possible (due to insufficient funds) the client will be notified of the result. If the deposit can proceed the client will be asked to confirm it. Only the person who originally executed the deposit will be able to confirm it. Once the confirmation has been made the external bank is queried to see if it is still able to withdraw the amount from the bank. At this point the deposit is made and the internal bank will show the new balance. If the withdraw failed then the client is notified of the result.

To withdraw money from the internal bank account the client will execute the bank manager, select the option to withdraw money and enter the amount to be withdrawn from the internal bank account. The control centre will process the transaction and request confirmation. Only the client making the withdrawal can confirm it. If the money requested is greater than the balance in the bank account you will be notified and the withdrawal will be cancelled. On confirming the withdraw the withdrawal will be made if the balance in the bank account is

still greater then the requested amount of the withdrawal.

All monetary transactions are stored in an audit file and logged. Should there be any discrepancy in the transaction, these files can be checked. It is possible to prove the initial monetary transaction as well as the confirmation of the monetary transaction. This, together with the fact that all monetary transactions are encrypted with the client's private key, provides the non-repudiation facility for all monetary transactions.

4.6 Advertisement viewing

To view advertisements and details of the advertisements is possible by both registered and unregistered clients. Two levels of advertisement viewing are provided. The first level of advertisement viewing is that of a short advertisement list which contains the advertisement number, a 70 character description of the advertisement and the cost per item being sold. This advertisement list can either be retrieved by using a software platform which is distributed to registered clients at registration time or can be retrieved by unregistered clients by downloading it from the control centre using anonymous FTP. The list which is created by the software application or obtained using FTP is a standard text file named STOCK.LST This file can be viewed using a standard text viewer. It is column formatted displaying the advertisement number, a description of the advertisement and a price per item being sold. The short stock list should be retrieved regularly as this list changes every time a stock item is sold out or a new advertisement is placed.

The second level of advertisement viewing shows more details of the advertisement. Details which are shown include the number of each item still available for sale as well as a full advertisement developed by the seller of the items for sale. The advertisements in the supported formats can be viewed by the client wishing to see more details of the advertisement. This facility is available to both registered and unregistered clients. Registered clients can request a detailed advertisement from any control centre while unregistered client can only request advertisements from the control centre to which it is communicating.

5 Security aspects of the system

This section argues that communication between the various modules is secure. Similarly, information storage at each of the modules is secure.

All transactions which are sent along the communications channel are encrypted using the RSA algorithm. Keys generated are never distributed publicly except for the public key of the control centre which is free knowledge to anyone wanting to communicate with it. The sales interface will keep a client's public keys while the client will keep the secret keys.

Transaction Parties	Encryption	Decryption
Sales interface →Registered client	Public key of client	Secret key of client
Registered client →Sales interface	Secret key of client.	Public key of client
Sales interface →Non-registered client	Secret key of sales interface	Public key of sales interface
Non-registered client →Sales interface	Public key of sales interface	Secret key of sales interface

Table 1: Key usage in transactions

The keys used in the encryption and decryption of the transactions are summarised in table 1.

5.1 Security aspects at sales interface

Only authorised people have access to the sales interface. These authorised people fall into two categories :-

- Registered clients are those users who have successfully completed a registration and have attained their interface applications which contain their unique secret RSA key.
- Nonregistered clients are guest clients that have downloaded interface applications from a server site. These clients are however limited to viewing advertisements only. Built into these applications is the public key of the control centre which is common knowledge to any application wishing to communicate with the control centre.

Secure storage

The storage of all critical data is encrypted and can only be viewed by the sales interface. Added security can be achieved by placing theses files in a high security area. The data which falls into this category of storage includes: security data, client data, bank data, transactions data and logs (for audit purposes). The logs consist of two parts. The first and most important is the actual message which identifies the transaction being made. This is generally the first identifiable part of any transaction. The next part of the log includes the confirmation of the transaction. With these facilities we are able to provide non-repudiation facilities to all parties in any of the transactions.

Non-secure storage

Non-secure storage is used for storing advertisements and other low risk data. These are not a security risk as the primary goal of the system is to allow as

many user as possible to have access to the advertisements. Apart from the advertisements there also exists client software which is made accessible to all clients registered and nonregistered. These files are not high risk and are also stored in this non-secure storage area. This area can also be viewed as the public area or the guest area for the domain. It is also possible to place other information here which is not a high security risk and should be accessible to anyone in the domain. Information such as operating instructions and registration instructions could be placed here. One of the most important files included in this area is that of the registration executable which must be downloaded and executed in order for a potential client to be registered.

5.2 Security aspects at client applications

Client applications for registered clients are distributed at registration time. Each set of client packages are unique. This is as a result of the embedding of the partial RSA secret key for that client. In order for the client to create the correct RSA secret key he must supply the correct PIN which he/she supplied at registration time. This PIN is not distributed in the application and thus is entirely secret to the client. To generate the correct RSA secret key the client package takes the partial RSA secret key that is found hard-coded into the application and combines it with the PIN supplied by the user. These two integrated make up the RSA secret key for the user. Part of the RSA secret key is therefore never made available and never stored at the client's package. An added advantage to this approach is that the client never needs to know his RSA secret key. He must however ensure that he uses only his own packages to interact with the control centre as they serve as a part of the authentication process. A client is restricted to communicate with the control centre successfully only by communicating with the relevant packages supplied to him at registration time and using the PIN which he supplied at registration time.

For potential clients that are not registered packages exist which can be downloaded from the control centre and executed. In these packages RSA public keys for the control centre are embedded. These, being public keys, do not pose a security threat if attained.

6 Conclusion

This paper described a prototype system that illustrates the use of a public network for personal financial and business transactions. It has been argued that the prototype system ensures secrecy, non-repudiation and the other guarantees required for acceptance of such a system. Apart from the normal encryption to ensure secure communication and storage, the fact that all (critical) transactions are verified minimise the potential of fraud. Additionally, dealing only

with known (registered) users further lessens the liklihood of fraud and serves as guarantee for the users (both buyers and sellers) of the system.

The use of self-contained modules, customised by the sales interface for an individual user, ensures that all technical aspects are hidden from the user. General consumer use of the system is therefore viable.

The current version of the prototype runs on a Novell local area network. MS-DOS versions of all the software modules have been demonstrated. These modules do not use any esoteric facilities of MS-DOS, and can therefore be ported to other operating systems without problems. User directories are currently used in place of electronic mail addresses as envisaged in the eventual prototype. However, this will also be easy to modify when the system is ported to the Internet.

References

[1] CP Pfleeger, *Security in Computing*, Prentice-Hall, 1989

[2] L Press, "Commercialization of the Internet", *Communications of the ACM*, **37**, 11, 17–21, 1994

[3] JR Vacca, "Mosaic: Beyond Net Surfing", *Byte*, **20**, 1, 75–86, 1995

[4] SH von Solms, "Information Security on the Electronic Superhighway", IFIP/SEC'96, Samos, Greece, 1996