Joint Conference of 1996 International Computer Symposium
December 19~21, Kaohsiung, Taiwan, R.O.C.

Design and Security Issues in Strongbox Systems for the Internet

(Extended Abstract)

Thomas Hardjono[1] and Jennifer Seberry

Centre for Computer Security Research
University of Wollongong, NSW 2522
Australia

Abstract

This paper presents and discusses some design and security issues surrounding electronic strongboxes *as an electronic counterpart of physical strongboxes typically found in large traditional financial institutions. The concept of electronic strongboxes is briefly discussed, comparing against physical strongboxes. A basic system for electronic strongboxes is then presented.*

1 Introduction

The growth of the Internet pushed by the development of user-friendly browsers has turned into reality the notion of electronic commerce and business on the Internet. The decrease in hardware costs and storage prices in the last few years has increased the accessibility of personal computers to the ordinary person on the street. Currently *Network Computers* (NC) are speculated as being the next possible source for large consumption of PC-related technologies, bringing not only electronic commerce, but a whole range of computerized activities and entertainment, into the home living room. New services will be provided via the Internet, connecting consumers and suppliers evermore closely in the global economy.

One such service will be that of *electronic strongboxes* [1] as part of the larger electronic commerce infrastructure. We view the provision of electronic strongboxes as a natural progression from that of electronic trading in general. As the security of the Internet is further developed and standards for electronic commerce become stable and are reflected in secure implementations, we perceive that electronic strongboxes will become "just another service" delivered through and by the Internet.

The concept of electronic strongboxes has been derived from the similar notion found in the physical world. In the traditional financial sector the provision of strongboxes has been in service for sometime. Customers can apply to have a private strongbox held within a bank, in which the customer can place any type and any amount of valuables, subject only to the physical characteristics of the strongbox. The bank typically has no interest in the contents of the strongbox, and derives income from providing safe storage and access to such strongboxes. The identity of the strongbox customer and the fact itself of the customer having a strongbox are usually treated as confidential by the bank.

The technology to implement secure electronic strongboxes is partly available today. Many of the required protocols can be derived from other proposed systems in electronic commerce, which so far has focused mainly on payment systems. These proposed systems range from those which require an interface to the existing financial infrastructure (such as DigiCash [2, 3], iKP [4], NetBill [5] and SET [6]), to those which employ electronic coins/cash as a reusable payment mechanism circulating electronically (eg. NetCash/NetCheque [7, 8]).

In the next section the background for electronic strongboxes is discussed. This is followed by a description of a basic system for electronic strongboxes in Section 3. The issues relating to design and to security are covered in Section 4. Some remarks are given at the close of the paper in Section 5.

2 Electronic Strongboxes

Physical strongboxes have been employed in the financial and other sectors for sometime now. Banks often provide strongboxes for their customers, charging a certain fee for the safekeeping of the strongboxes. Typically, some form of identification – direct or indirect – is required before the bank allows the customer access to the box itself. The identification can be an actual identifying personal information (eg. driver's license), or it can be in the form of a token (eg. card or access-key) recognizable by the bank. The advantage of a token lies in the *anonymity* of the customer, which is a primary requirement for physical strongbox and electronic strongbox systems.

The requirement of anonymity is tied closely to that of privacy, and is accepted as part of the service provided by the bank or other strongbox providers. In the electronic realm, anonymity has been a major issue within electronic commerce dealing with monetary transactions. Like ordinary cash, electronic

[1] The first author is also at the University of Western Sydney - Macarthur, NSW 2560, Australia.

money should provide the basic features of the untraceability of payments, undeniability of payments (and receipts), and others.

In the electronic strongbox concept, the anonymity of customers goes hand-in-hand with the need of secrecy with regards to the "electronic items" being stored in the strongbox. Like the bank, the electronic strongbox provider should not be interested in the contents of the strongboxes, but should derive income from providing a user-friendly and secure strongbox service. With the advent of browsers for the world-wide-web, and the resulting interest in electronic commerce, user-friendly interfaces can be created using secure browsers that have been implemented to handle electronic commerce and trading.

Users of a strongbox-browser should be allowed to manipulate objects stored within the strongbox using an iconic object representation. These electronic objects or items can be certified representations of physical objects, and can include electronic coins or cash, electronic bank cheques, digital documents (eg. stocks and contracts), anonymous digital certificates of ownership of physical items, cryptographic material to access other services, and others. A customer may have multiple strongboxes, each at differing strongbox providers. Joint ownership of a strongbox can serve as an exchange medium between its two owners. Using a unified interface, customers should be able to move items between strongboxes, each under different providers.

The provision of strongboxes on a global network such as the Internet should lead to an economy which is based not only on monetary transactions, but also on *barter*, or personal trade. As the exchange of items is a normal part of daily life, electronic strongboxes can be a medium within which to carry-out non-monetary commerce with privacy, confidentiality and user anonymity. Other institutions may act as *valuers* and *converters* where legal and valuable items (eg. gold) are given a valuation and electronic certificates are generated for the items. The same institution may also provide long-term safe storage for the physical items, whilst the anonymous owner uses the electronic certificate on the Internet. Private purchases of legal items between users should be facilitated as such an event is common in everyday life.

Another way of approaching the electronic strongbox concept is that of seeing the strongboxes as a kind of *secure public storage* medium. Items belonging to a user can be dispersed throughout the Internet in a transparent manner. Users should not be concerned with the underlying management of the strongboxes. However, they should receive a high level of assurance that the contents of the strongbox will not be visible to other people and that the items will not be stolen.

Previous research on anonymous and verifiable databases have been conducted by Brandt *et al* [9], and also reported in [10]. The aim in [9] was to allow certain institutions (eg. hospitals) to maintain data about people (eg. patients) whilst maintaining anonymity through the use of *pseudonyms* [11] for privacy reasons. Persons having data in the database could verify that their information is correct and that no illegal modifications had been made.

This is significantly different from the notion of electronic strongboxes. First, the items stored in the strongboxes carry real and global value as they are an electronic representation of physical goods. Secondly, the items themselves can circulate within the system, moving from one strongbox to another. Thirdly, such a movement of items should be untraceable, as the ownership of an item is regarded as confidential information. Finally, although anonymity is equally required as in [9], in electronic strongboxes it represents a more complex problem as it involves several parties - similar to electronic payment systems.

3 Basic Components

Figure 1 illustrates a simple design for a strongbox system, borrowing the terminology from the area of electronic payment systems. All electronic interactions between participants are assumed to be over a secure channel, with peer authentication conducted at the commencement of communications. The proposed system of Figure 1 does not pretend to be comprehensive, and it attempts only to address the main components only. Additional components will be required to support the framework to achieve full workability.

The participants of the system are as follows:

- *Customer*: the customer or user, interacting with the Strongbox Provider (eg. Bank) for the safekeeping of electronic items.
- *Strongbox Provider*: an institution that provides the electronic strongbox service to a customer, accepting the storage and retrieval of electronic items to/from the electronic strongboxes.
- *Valuer*: the on-line Valuer is trusted to verify that an electronic item belonging to an owner (ie. Customer) truly exists and has not been modified by its current owner. The Valuer can also be requested to split items into several sub-items, and issue certificates for them. Several Valuers may exist on-line, and each must recognize the other's certification.
- *Exchange Facilitator*: the Exchange Facilitator aids two or more Customers who wish to exchange items from their strongboxes. The Facilitator can be a Strongbox Provider and is under the jurisdiction of the Association.
- *Association*: the Strongbox Providers and the Valuer work under the umbrella of the Association. Customers bring disputes to the Association.

In addition, there are the *Physical Valuer* and the *Notary* which are in the physical world and interfaced to the electronic world. The Physical Valuer should be distinct from the on-line Valuer as the Physical Valuer knows what a physical item is and which pseudonym forwarded the physical item to be valued. The Physical Valuer stores the physical items at the *Secure Physical Storage*, to which the Association has access in the case of disputes. The Notary comes in on behalf of a Customer when disputes necessitates their

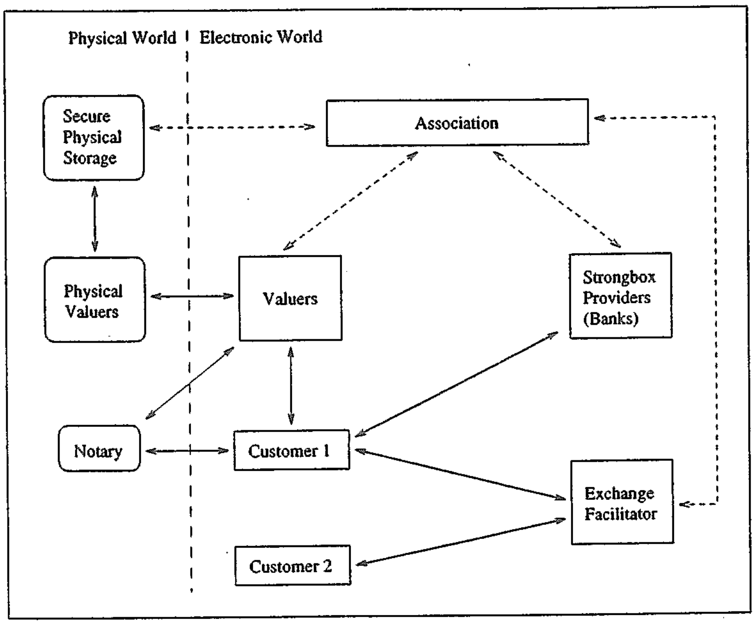

Figure 1: An Electronic Strongbox System

presence. In the remainder of this paper the term "Valuer" alone will refer to the on-line Valuer (as opposed to the Physical Valuer).

The Customer is the owner of the contents of a strongbox and is deemed also as the owner of the strongbox. The Customer must first join the strongbox system by opening an account with the Strongbox Provider, which can be a Bank or other institutions having the necessary computer infrastructure to provide this service. The Customer obtains membership through the Association which issues the Customer with the credentials (eg. within a smartcard) and with a pseudonym to be used within the system. The Customer henceforth employs this pseudonym when using the system.

4 Design and Security Issues

There are a number of issues relating to the design of electronic strongboxes and those relating specifically to the security of strongbox systems. Some of these issues are briefly discussed together in the following.

4.1 Anonymity and Untraceability

Although we assume that smartcards will be employed within the strongbox system, anonymity of Customers remains a difficult problem. Anonymity must be provided at the system-wide level, which may extend over national boundaries. A Customer may have several strongboxes under different Strongbox Providers, and he or she must be able to move items between these strongboxes, all the time maintaining anonymity and untraceability of items. Hence, untraceability is closely linked to Customer anonymity. Once an item is legally within the system, its current whereabout (ie. in which strongbox) within the system must be unknown.

The problem of Customer anonymity and item untraceability is somewhat exacerbated with the functional requirement that legal and indisputable (non-repudiated) item exchanges be possible within the system. Here, the Exchange Facilitator must ensure that item exchanges are free from possible cheating by either parties.

4.2 Representation of Electronic Items

There are a number of ways that items can be represented in electronic form. In order to allow for negotiations before any item exchanges and to allow a Customer to prove ownership of an item without the risk loss (ie. stolen) or fraud, we propose the use of two certificates for each item:

- *Item Certificate*: this is the electronic item itself in the shape of an unforgeable certificate and having a one-to-one correspondence with the physical item. The Item Certificate carries the signature of the Physical Valuer and is co-signed by an on-line Valuer. No pseudonym is mentioned in this certificate.

- *Description Certificate*: this is a certificate guaranteeing that a given item exists somewhere in the system. The certificate contains a digest or hash of the Item Certificate, and is signed by the on-line Valuer. The certificate may contain the pseudonym of the current owner.

The concept is derived from the idea of certified photocopies of important documents (eg. passports) which are often required for government and legal purposes. The two certificates are inseparable and should be stored in the strongboxes. The aim of having a Description Certificate is to allow one Customer to prove its ownership to another Customer before an exchange occurs. During an exchange, both certificates are handed-over as an item unit.

Similar to electronic cash, some form of serial numbering may be applied to all electronic items system-wide, to prevent illegal copying of certified items by its current owner. This must be done with the precaution that the serial numbers do not become way to trace the movement of items [12].

Upon an exchange between two Customers the Exchange Facilitator may request an on-line Valuer to re-certify electronic items as belonging to their new owners respectively. For each electronic item, both the Item Certificate and the Description Certificate must be signed by the on-line Valuer. The Description Certificate will then contain the pseudonym of the new owner of the corresponding item.

Note that no identity information, such as the pseudonym, is mentioned anywhere within the Item Certificate. Thus, the current owner of the Item Certificate may at any time obtain the actual physical item by presenting the Item Certificate to the Physical Valuer. The physical Valuer must then inform the on-line Valuer of the removal of the item from circulation within the electronic world.

4.3 Item Storage and Types of Access

Electronic items (in the form of Item Certificates and Description Certificates) must be stored encrypted within the strongbox. The owner can use a symmetric cryptosystem with a private key known only to the owner and stored within the owner's smartcard. An (encrypted) index of items within a strongbox may be inserted into the strongbox by the owner to aid him or her in retrieving only certain items.

The encipherment of individual items by a Customer/owner lends to two possible ways of accessing the strongbox:

- *Strongbox access by the Customer.* Here it is the Customer that enciphers and deciphers the string corresponding to the strongbox. When a Customer presents his/her identifier during the authentication process, the Provider simply passes the Customer his/her strongbox via the secure channel. The Customer "opens" (deciphers) the strongbox using the secret key known to the Customer alone, and either inserts or removes items from the overall collection.

  If each individual item in the strongbox is also enciphered, a Customer should first extract an index of items stored in a particular strongbox. Only then should the Customer insert/remove specific items.

- *Strongbox access by the Provider on behalf of the Customer.* If a higher level of trust exists between the Customer and the Provider, the Customer can relegate the task of opening and closing the strongbox to the Provider. Using the secure channel the Provider can deliver the index of items to the Customer, from which the Customer can select items or insert new items.

  Notice here that this is equivalent to the Provider having the access key to a Customer's strongbox and having the capacity to alter or damage the (encrypted) items. This possibility must be weighed against the trust level accorded to the Provider.

  Although this approach has more risks, some methods to limits such risks can be employed. Thus, for example, the Provider can give a copy of the strongbox index which is signed by the Provider. The index can be given both at the opening and closing of a strongbox. Hence, using this index the Customer can challenge the Provider, should some items go missing from the strongbox.

In practice a Customer may insert any data string into a strongbox, subject only to storage space on the part of the Provider. However, such data strings will not have been certified by any Valuer, and thus would not be usable in any legal (disputable) exchanges.

4.4 Against Losses

An interesting notion is that of having *backups* for strongboxes. In accordance with requirements of electronic strongboxes [1] and the norms found in physical strongbox systems, a Provider should not know the contents of a given strongbox (nor the value of the items in it). To safeguard the Provider from any damaging claims by a Customer, two possible solutions can be employed:

- The two parties can agree upon an upper limit in monetary terms of the possible claims made against the Provider by a Customer. This is similar to insurance against losses.

- The Provider can make a backup of a strongbox immediately before a strongbox is released upon a check-out request by a Customer. Should there be some protocol failure leading to the loss or corruption of the strongbox, the Provider can bring the backup copy on-line.

  Note that additional means (eg. serial numbering) should be used to ensure that a Provider does not make illegal copies of strongboxes and that only a single strongbox is ever valid on the system.

  To prove the authenticity of that single strongbox copy, a hash of the concatenation of the Strongbox and the previous Receipt (previously issued when the Customer last checked-in his/her strongbox) can be created and signed by the Provider, and then delivered to some third party (eg. notary) with an attached lifetime.

5 Remarks and Conclusion

In this paper we have briefly discussed some of the issues for the design of a secure electronic strongbox system for the Internet. The basic components and requirements of a strongbox system has been presented, focusing only on the main components of the system, namely the Customer, Strongbox Provider, the Valuers and the Exchange Facilitator. This effort does not pretend to be comprehensive, as there are a number of other issues that remain to be resolved in the wider context of electronic commerce, and also within the specific scope of electronic strongboxes.

Further work will follow in defining precise terms and the protocols for the strongbox system. In addition, further investigation must be carried-out into the suitability of some of the components implementing electronic commerce for use in strongbox systems. The aim here is to seamlessly integrate strongbox systems with the larger infrastructure for electronic commerce. This would lead strongbox systems to be eventually viewed as simply a service given through and by the Internet.

References

[1] T. Hardjono and J. Seberry, "Strongboxes for electronic commerce," in *Proceedings of the 1996 Usenix Workshop on Electronic Commerce*, Usenix, 1996. (to appear).

[2] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Communications of the ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[3] D. Chaum, "Achieving electronic privacy," *Scientific American*, pp. 96–101, August 1992.

[4] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, and M. Waidner, "iKP – a family of secure electronic payment protocols," in *Proceedings of the First USENIX Workshop on Electronic Commerce*, (New York), USENIX, 1995.

[5] M. Sirbu and J. D. Tygar, "NetBill: An internet commerce system optimized for network-delivered services," *IEEE Personal Communications*, pp. 34–39, August 1995.

[6] Visa and MasterCard, "Secure Electronic Transaction," 1995. http://www.visa.com.

[7] B. C. Neuman and G. Medvinsky, "Requirements for network payment: The NetCheque perspective," in *Proceedings of IEEE Compcon'95*, (San Francisco), IEEE, 1995.

[8] G. Medvinsky and B. C. Neuman, "NetCash: A design for practical electronic currency on the internet," in *Proceedings of the First ACM Conference on Computer and Communications Security*, ACM, November 1993.

[9] J. Brandt, I. B. Damgard, and P. Landrock, "Anonymous and verifiable registration in databases," in *Advances in Cryptology - Proceedings EUROCRYPT '88 (Lecture Notes in Computer Science No. 330)* (C. G. Gunther, ed.), pp. 167–176, Springer-Verlag, 1988.

[10] T. Hardjono and J. Seberry, "Applications of smartcards for anonymous and verifiable databases," *Computers & Security*, vol. 14, no. 5, pp. 465–472, 1995.

[11] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[12] D. Chaum, "Privacy protected payments: Unconditional payer and/or payee untraceability," in *Smart Card 2000: The Future of IC Cards* (D. Chaum and I. Schaümuller-Bichl, eds.), pp. 69–93, Amsterdam: North-Holland, 1989.