1996

Design and security issues in strongbox systems for the internet

Thomas Hardjono

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Design and security issues in strongbox systems for the internet

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 provided and the functional and security requirements of the system's components is presented.

Publication Details

Hardjono T and Seberry J, Design and security issues in strongbox systems for the internet, Proceedings of the 1996 International Conference on Cryptology and Information Security, Kaohsiung, Taiwan, 19-21 December, 1996, 99-103.

Design and Security Issues in Strongbox Systems for the Internet

(Extended Abstract)

Thomas Hardjono and Jennifer Seberry

Centre for Computer Security Research
University of Wollongong
Wollongong, NSW 2522
AUSTRALIA
Tel: +61-42-213859
Fax: +61-42-214329
email: thomas/jennie@cs.uow.edu.au

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 provided and the functional and security requirements of the system's components is presented.

Keywords: Electronic Strongboxes, Electronic Commerce, Payment Systems, Distributed Systems.

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 being flagged as 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. A whole range of 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 implementation, 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 party available today. A large part of the protocols that can be employed can be derived from other 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]).

2 Electronic Strongboxes: Background

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 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 existing 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. Using a unified interface, customers should be able to move items between strongboxes, each under different providers.

A third party maybe appointed for such cases when disputes occur between an owner of a strongbox and the institution that maintains the strongbox. This may occur, for example, when a dishonest user claims that his or her access key has a matching strongbox within the bank, or when the bank inappropriately denies access to a valid owner of strongbox.

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 valuable items (eg. gold) are given a valuation and an electronic certificate for the item is provided. 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. Such certificates should never be convertible to electronic coins or cash for payments, as they may present an opportunity for money laundering or similar activities that may have drastic implications on the Internet-based economy.

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.

The early work by Brandt *et al* [9] points to the benefits of anonymous and verifiable database, particularly in the context of privacy against government bodies that wish to cross-correlate data belonging to individuals in society. In [9] the true identity of each individual remains unknown and the individual employed a different *pseudonym* [10] when dealing with each government body or institution. The main feature of the work was that each individual must also have the ability to verify that his or her personal details held by an institution are correct. Further work has also been reported in [11].

However, one underlying difference between the anonymous/verifiable database and the public strongbox concept is the privacy of data. In the anonymous/verifiable database, it is intended that the institution that maintains the database view the data belonging to the users, whilst at the same time maintaining the anonymity of the users. The users can then verify that the database contains correct data about the user (eg. patient record in a hospital system). In contrast, in the public strongbox concept the contents of the strongbox must remain confidential, with the users still remaining anonymous and being able to verify the contents of the strongbox.

3 Strongbox Systems: 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

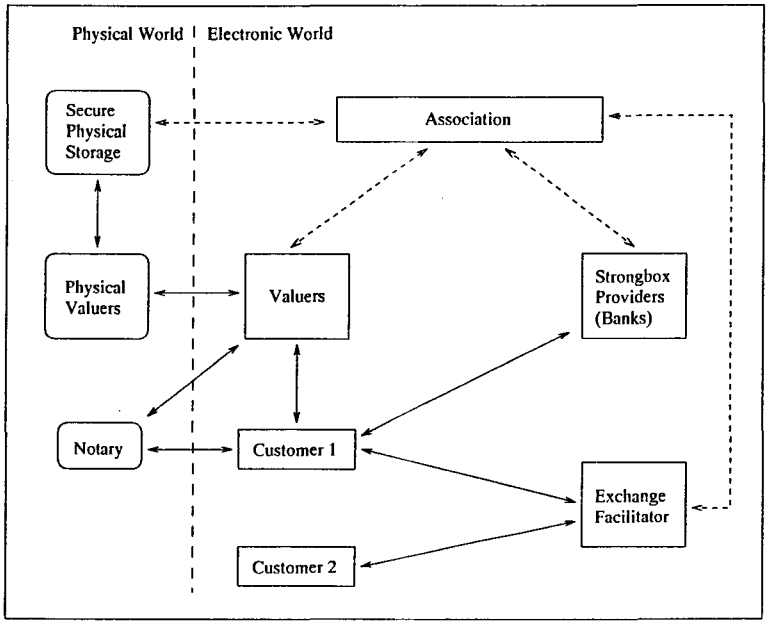

Figure 1: An Electronic Strongbox System

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 presence [1].

[1] In the remainder of this paper, unless otherwise stated, the term "Valuer" 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

4.1 Representation of Electronic Items

The representation of items electronically can take two forms, bearing in mind the needs of the items to be valued or exchanged:

- *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.
- *Description Certificate*: this is a certificate guaranteeing that a given item exists somewhere in the system. The certificate may contain 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 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.

The concept is derived from the idea of certified photocopies of important documents (eg. passports) which are often required for government and legal purposes. Periodically the Description Certificate must be renewed by way of the Item Certificate being reconfirmed by the on-line Valuer.

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.

4.2 Strongboxes

Bearing in mind that electronic items take the form of certificates, a strongbox can implemented by an organized enciphering the collection of (indexed) certificates belonging to the Customer. Two general approaches to accessing strongboxes can be followed depending on the level of trust accorded by the Customer to the Provider:

- *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 the Customer trusts the Provider, the Customer can relegate the task of opening/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 the strongbox contents.

  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.

There are a number of further requirements that must be fulfilled by any strongbox system. Some of these are derived from concept in electronic payment systems in general, while some are specific to electronic strongboxes:

- *Privacy of strongbox contents.* As in the case of physical strongboxes, the contents of the strongbox should remain undisclosed to all parties except the key holder opening it using a valid key. Any system implementing the strongbox should ensure that the institution providing the service does not have back-door or other hidden channels to access or view the contents of the electronic strongbox.

  In the physical world, some level of trust exists between the bank and strongbox owner, whereby the owner relies on the bank not to place hidden cameras designed to view the strongbox contents and that the bank will not tamper with the strongbox. Ideally, such trust should also exist between a customer and the strongbox provider, similar to the level of trust between merchant and acquirer [4, 6].

- *Privacy of strongbox locations.* A user may have multiple strongboxes scattered all over the Internet under different guarding institutions. The locations of these strongboxes should be private information, available only to the owner (or any other delegated user) and the respective institutions.

- *Access to strongbox only by key holder.* The institution must without exception provide access to the strongbox only to the key holder that presents a valid key. A security mechanism must be employed to provide at least two levels of verification, namely at the point of request for access to the strongbox, and later at the point of the opening strongboxes. These two levels can be implemented cryptographically, and should eliminate possibilities of procedural errors.

- *Storage of a variety of electronic items.* A strongbox should be able to store a variety of digital items, subject only to the agreed storage space limitations. Even such limitations should be easily and immediately negotiable when a user reaches his or her storage limit, as the price for secondary storage continues to drop. System parameters that protect the strongboxes must be maintained under secure and tamper-free storage at the institution.

- *Items exchangeable between strongboxes.* Analogous to the physical counterpart, electronic strongboxes must allow for the exchange of items between two (or

more) strongboxes. Strongboxes may belong to the same owner, or they may belong to different owners who are working together.

- *Untraceability of moved items.* Since the contents of strongboxes must remain private, moved items must then be untraceable. Untraceability should hold regardless of how many times an item has been moved between strongboxes, and regardless whether or not the item finds its way into a strongbox within which it previously resided. That is, a strongbox should not have a "memory" of its previous contents.

- *Strongbox key can be delegated.* Similar to the physical strongboxes, any person carrying the appropriate key must be able to open the box. Ideally strongboxes should even allow stolen keys to be used, as the issue of protecting keys is separate from user anonymity.

  In electronic strongboxes, delegation must be provided, whereby an owner of the strongbox can delegate another user to become a key holder to access the owner's strongbox. Both users must remain anonymous. At the same time, delegation schemes must have a limited lifetime or the ability to be revoked by the owner [13].

  Single-use keys may provide a solution, in which delegated keys are derived from the original key, and where the bank holding the strongbox are aware of a key being a derivative, and would allow only one-off access to a given strongbox. Multiple-use keys may also be devised, using technology similar to electronic coins. Every usage of the key would reduce its worthiness, until it is diminished when it reaches its maximum number of usages.

- *Strongboxes movable to other institutions.* Strongboxes must be movable between institutions, similar to the way electronic cash or coins are movable around the Internet. An owner of a strongbox must be able either to move the entire strongbox without opening it, or to shift the contents of one strongbox at one institution to another strongbox under a different institution. Both alternatives are attractive, and both should be available to the user, depending on the user's circumstances. Security, privacy and anonymity must be ensured in both cases.

4.3 Strongbox Providers

Similar to financial institutions in electronic payment systems, Strongbox Providers face a range of possible functional and security failures that may affect the reputation of the Provider. However, unlike Internet-based cash or payment systems, the

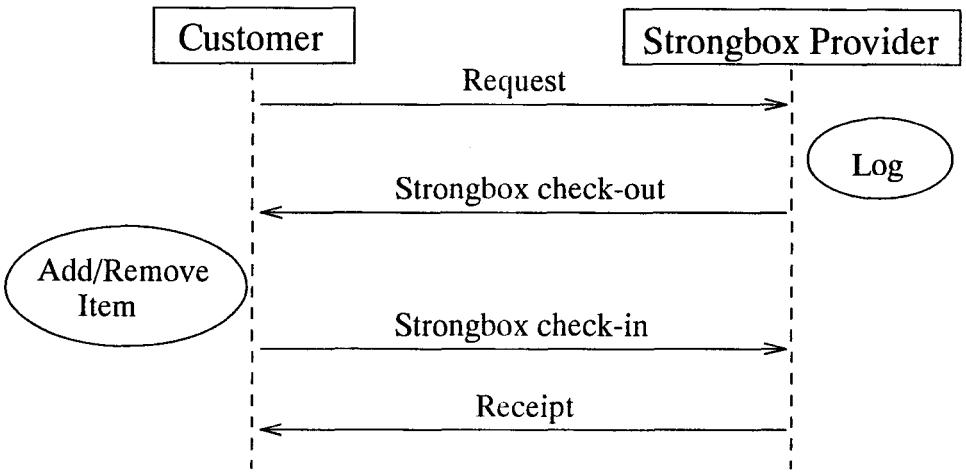

Figure 2: Check-in and check-out of electronic strongboxes

scenario for fraud by the Customers (or by a Provider) are somewhat reduced. Once a strongbox is checked-in, the responsibility against any fraud lies at the door of the Provider. Thus, there are some basic requirements which must be satisfied for the secure working of a strongbox system:

- *Proof of the retrieval of a strongbox.* The Provider must have some form of proof that a strongbox is currently being "checked-out" (Figure 2). That is, that the strongbox has been retrieved and is currently in the possession of the Customer. This is to prevent the Customer from claiming otherwise and therefore forcing the Provider to take account of losses. This notion is similar to that of the forging of electronic cash or coins, or to that of denying that payments have or have not been made.

  The retrieve and store operations must exhibit the typical transaction properties of atomicity, consistency, isolation and durability [14, 15].

  A further aspect that must be taken into consideration is the allowable length of time for a strongbox to be held (checked-out) by its owner and the implications on security. Given that a Customer typically knows the contents of his or her strongbox – either from human memory or through a list stored securely (eg. smartcard) – it is reasonable to assume that the check-out and check-in should occur within the span of a single transaction. The notion of time here is again similar to that found in electronic payment schemes, in which a merchant expects some level of immediacy in the payment by a customer.

- *Verification of access key to the strongbox.* Before providing a key holder with access to the claimed strongbox, the Provider must have sufficient proof that the requester (ie. owner or their delegate) is a valid party within the system. That is, the requester has a valid pseudonym and can be authenticated. The

Provider must also verify that the key is a recognized and valid key.

One potential problem would be the possibility of the illegal duplication of access information. That is, the potential that more than one access key exists at any time. Current technology can solve this problem either through smartcard systems or through the provision of a single-use access keys for the strongboxes. In the later case, a new access key needs to be generated each time a strongbox is retrieved and stored.

An interesting notion is that of having *backups* for strongboxes. In accordance with previous requirements and the norms found in physical strongbox systems, a Provider does 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 a Customer complain or 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 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 by the Provider and delivered to some third party (eg. notary) with an attached lifetime.

4.4 Customers

From the Customer's point of view the Provider is the best point of attack both from external attacker and from within the Provider institutions itself. Thus, there are a number of requirements that need to be satisfied:

- *Anonymity of owner.* The owner must remain anonymous, and the fact that she or he owns a strongbox must also remain a private fact. Methods to create pseudonyms exist in other forms of electronic commerce which can be used in the strongbox case.

- *Anonymity of key holder.* The key holder is the user that presents a valid key to the Provider to access a strongbox held by the Provider. The Provider has the right to verify that the key fits into one of its strongboxes, and to deny access if the verification fails. Depending on the system, this must be without the Customer necessarily revealing the actual key (eg. zero-knowledge-based solutions). The key holder can be the owner of the strongbox, or any other user delegated to access the strongbox by its owner.

- *Unauthorized retrieval of strongbox is impossible.* A Customer must have the assurance that the unauthorized checking-out of his or her strongbox is impossible. Unlike electronic cash, electronic items which are stolen cannot be easily replaced as the items may have been exchanged through a number of hands.

  A possible safe-guard can be implemented at the physical end, when Customers convert their electronic items back into physical items currently being stored in the secure physical storage. Even then, disputes may occur between the current holder of the electronic item and those who claim that it was stolen from them.

- *Proof of storage by the Provider.* A Customer requires some proof in the form of a *receipt* that his or her strongbox has been correctly checked-in and that the Provider now holds the strongbox.

- *Proof of valuation.* When an item undergoes valuation or when an item is split by the Valuer into several electronic sub-items, a Customer owning the item (and thus sub-items) requires proof in the form of the certification of the item (sub-items). Clearly the Valuer itself must be a certified one and be authenticated by the Customer before any valuation transaction occur.

- *Proof of exchange transaction.* When a Customer carries-out an exchange of items with another Customer via the Exchange Facilitator, both Customers must have sufficient proof that the exchange occurred correctly in such a way that neither party can deny the transaction.

4.5 On-Line Valuers

In order to bring an item into the system the Customer must first obtain a valuation of the physical item to the Physical Valuer. The Physical Valuer issues the Customer with a digital certificate corresponding to the physical item. This certificate is recognized and accepted by all participants in the system. The actual physical item itself is then stored in the Secure Physical Storage, under the control of either the physical Valuer or of the Association. Any Customer presenting an electronic certificate for a physical item can obtain the item from the Physical Valuer or through the Association.

The unit of the physical item to be valued and certified must be agreed upon between the Customer and the Physical Valuer (eg. six bars of gold can be written under one certificate, or six certificates can be produced corresponding to the six physical items). Having small units for the valuation allows for easier usage of the items at a later date. However, should a Customer wish to break-up an electronic item into several reasonable components – bearing in mind the physical reality of the item – the Customer can approach the on-line Valuer to obtain such services.

Once within the system the certificate is referred to as an electronic item. What the item is and who holds the item presently must remain confidential. A Customer can store the electronic item with any Strongbox Provider, assuming he or she already has a strongbox account with them.

For each valued item and valuation result it is important that the Valuer obtains proof of receipt from the Customer. This is to prevent a Customer accusing the on-line Valuer of stealing an item submitted for valuation.

4.6 Exchange Facilitator

When two or more Customers have agreed to exchange items, they can carry-out the exchange of the corresponding electronic items through the Exchange Facilitator (Figure 3). Ideally, before an exchange occurs, the Customers should prove the possession of the items to each other. This can be done via the *Description Certificate* which contains the pseudonym of the owner and which has been signed by a Valuer.

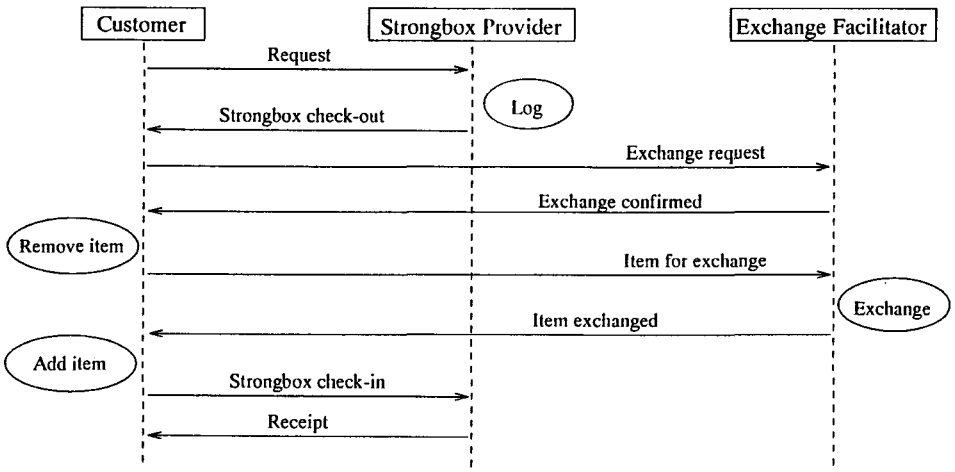

Figure 3: Exchange of electronic items

However, even without such pre-exchange confirmation of possession, the Exchange Facilitator must be able to ensure that no cheating occurs. The Facilitator must inform each Customer as to the electronic items it has received for the exchange

instance (to prevent cheating), and the Facilitator must also provide a guarantee of non-repudiation should one (or both) Customer dispute the exchange. The Facilitator can be a trusted third party, or it can be one of the Strongbox Providers selected by both Customers.

The use of the Exchange Facilitator is optional. Customers can perform any exchange of items directly among themselves, through a secure channel. However, without the Exchange Facilitator disputes cannot be resolved and the burden of risks lie fully with the Customers.

Corresponding to the proofs required by a Customer for the exchange of an item, the Facilitator requires proof of the submission of the items to be exchanged, and more importantly proof of the delivery and receipt of the items after the exchange. This proof must come from all involved Customers, and serves as protection for the Facilitator against false claims by the Customers.

5 Remarks and Conclusion

In this paper we have briefly discussed 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 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. This should lead to a seamless integration of strongbox systems into the larger infrastructure for electronic commerce. This would further allow strongbox systems to eventually be viewed a 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. `http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/`.

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

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

[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.

[13] M. Abadi, M. Burrows, C. Kaufman, and B. Lampson, "Authentication and delegation with smart-cards," Technical Report 67, Digital Systems Research Center, October 1990.

[14] L. J. Camp, M. Sirbu, and J. D. Tygar, "Token and notational money in electronic commerce," in *Proceedings of the First USENIX Workshop on Electronic Commerce*, (New York), USENIX, 1995.

[15] L. Tang, "Verifiable transaction atomicity for electronic payment protocols," in *Proceedings of 1996 IEEE ICDCS16 International Conference on Distributed Computing System*, IEEE, May 1996.