A Secure Electronic Payment Scheme for Charity Donations

Mansour A. Al-Meaither* and Chris J. Mitchell

Information Security Group, Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, United Kingdom
{M.Al-Meaither, C.Mitchell}@rhul.ac.uk

Abstract. Although many charities have a web presence, almost all of them have been designed to accept credit cards as the only means for making donations. The anonymity requirements of many donors, however, make the existing means of donation inappropriate for them. In this paper we investigate the business need for an internet charity donation scheme, identify the security requirements such a scheme should fulfill, and propose a scheme that uses an anonymous electronic cash technique to make donations, and that employs smart cards for donation distribution. Finally, we analyse how the proposed scheme matches the identified security requirements.

Keywords:

charity, e-commerce security, payment systems, anonymity, smart cards.

1 Introduction

Giving charity is a common activity for many individuals; for instance giving charity is an integral part of the Islamic faith. One occasion for making charitable donations is the month of Ramadan, where, after completing a month of fasting, Muslims celebrate Eid, the festival of the breaking of the fast. It is also an occasion to make a special donation to the poor. All Muslims who have enough money to take care of their own family's needs must make this donation. The amount of donation is the same regardless of their income.

On the other hand, the Internet and e-commerce are changing individual lives considerably. The Internet excels at facilitating the exchange of information and goods, and what better use for this exchange than giving to those in need? With the ever growing popularity of the Internet, the transition from traditional commerce to electronic commerce is becoming a reality. This transition is supported by the convenience, speed and ease of use of the new commerce scenarios. Electronic payments are a crucial component in the development of e-commerce.

* This author's work is supported by the Saudi Arabian Government

Although the necessary technology is already in place, most charities do not take advantage of the ubiquity of the Internet and recent developments in smart card technology. However, individuals are increasingly prepared to donate online. According to [3], of those Internet users who are likely to make a donation online, 52% have purchased a product or service over the Internet, making online buyers more likely to give online than other Internet users.

Currently, almost all online donation mechanisms found on charity Web sites are based on electronic credit card transactions. This is a potential problem since these systems do not provide any anonymity to the donor. Privacy concerns are a barrier to online donations just as they have been for e-commerce transactions. According to [3], concerns about privacy and credit card security remain high. 71% of donors said they were concerned about the security of their personal information online. Nearly 90% said they would never give their credit card information out to a charity. The current situation could be changed if a new electronic payment scheme for charity donations can be devised.

In this paper, we introduce the concept of e-donation, the electronic counterpart of a charity donation. We propose a scheme that allows donations to be made anonymously and distributed to recipients using smart cards, allowing recipients to redeem their e-donations directly from a shop. In particular the scheme involves the donor contributing a specific amount of money to the charity, which then arranges for the recipient to receive goods of precisely the value contributed by the donor. Moreover the donor can specify the nature of the goods to be made available to the recipient. Whilst this is not a model of charitable donation of general applicability, it matches the particular requirements of certain scenarios, e.g. the obligation on Muslims to make donations during Eid (as described above).

2 System Model

In this section, we describe our model for Internet charity transactions. The model identifies the entities involved and includes a brief description of their interactions.

2.1 Participants

We now examine each of the participants in an electronic payment scheme for charitable donations.

- **Donor**: A person who wishes to donate to a charity anonymously using the Internet.
- **Charity**: A charity is an intermediary between the donor and the recipient. It generates and issues e-donations to the recipients. It trusts the Pseudonym Server to issue valid electronic coins to the donors.
- **Recipient**: A recipient is the entity that receives goods when redeeming an e-donation from a participating store. Each recipient has a smart card supplied by his charity. This card holds e-donations (specifying particular goods)

issued by the charity which the holder can redeem from a participating store at a convenient time.

- **Store**: A store is an entity willing to promote its goods through participation in the scheme. It has an agreement with a charity to exchange e-donations generated by that charity for goods described in the e-donations. It uses a terminal to receive e-donations from the recipient smart card.
- **Certification authority (CA)**: A trusted entity that generates public key certificates for charities, stores, and the pseudonym server.
- **Pseudonym server (PS)**: A trusted entity that will bind cryptographic data to participants. It provides an infrastructure for issuing anonymous identities and electronic coins to donors. It is trusted not to revoke the anonymity of a donor at any time except under certain conditions agreed upon by all participants. It is trusted by all other parties and should be managed in such a way that fraud is very unlikely. To cover the operational costs of providing this kind of service, the PS might make a charge to the donor and/or the charity.

Trust is a critical issue in payment systems. In our model, we assume that the store and the charity trust each other. This trust is explicit as the store and the charity have a formally established agreement that defines the trust and liability relationship. The donor trusts the charity to deliver his donation to a deserving recipient. The donor might need a receipt for his donation from the charity to prove it has been issued to a recipient. All participants trust the CA and the PS to be honest.

2.2 Interactions

E-donation will provide a recipient of charity with the digital representation of a right to claim goods of a specified type from a participating store. A participating store will first need to decide which types of goods it will make available for distribution via charitable means — for each such item it will generate an e-donation token. Each such token is a simple data structure containing a description of the goods to be purchased. Associated with each token will also be the cost for a donor to purchase a right for a recipient to receive the goods specified in the token. The charity publishes these e-donation tokens via its web site. When a donor wishes to donate, he first contacts the PS to get an electronic cash coin which can only be used to donate to a charity, and an anonymous identity (pseudonym) used when communicating with a charity. After selecting the kind of donation he wishes to make at a charity web site, the donor makes the donation using the electronic cash coin received earlier from the PS. In response the charity generates an e-donation that satisfies the donor requirements and keeps it in a database.

When the charity decides to issue an e-donation to a recipient, it retrieves this e-donation from the database and loads it into the recipient's smart card. The recipient collects the goods from a participating store in exchange for the e-donation contained in the smart card. At a later stage, the store sends all the redeemed e-donations to their respective charities for clearing.

A great advantage of our scheme is transparency, i.e. the donor knows that a recipient will receive goods exactly as specified by the donor. Moreover, the charity does not need to be contacted during each redemption.

3 Security requirements

The purpose of the scheme is to facilitate the transfer of donations from donors to recipients. However, the scheme provides the potential for considerable financial gains for those who attack it successfully. Therefore security measures must be provided to protect the e-donation transactions. We discuss the security requirements that our scheme should satisfy.

3.1 Donor Anonymity

When it comes to charity donations, donor privacy is important. This is especially important in an internet environment where information may travel through network segments that are not necessarily trusted. The donor wants anonymity for his donation; neither the charity nor the recipient should be able to learn the donor's real identity. There are many reasons why anonymity might be required in a payment system [2]; in this case, the donor might not wish charities to be able to link different donations together and build a profile of his/her behaviour.

However, there are situations where anonymous payments can be misused for criminal activities [6]. Furthermore, there may be regulatory and legal constraints limiting anonymous donations. In order to make an anonymous electronic charity payment system acceptable to both donors and governments, a mechanism for limiting donor anonymity may also be needed.

3.2 Double spending

Double spending refers to the possibility of fraudulently spending the same e-donation more than once. Since e-donations are in digital form, they can readily be duplicated by the store or by the recipient, who may also blame each other for any fraudulent behaviour. If double spending does take place, the charity will not know this until the stores send the redeemed e-donations for clearing.

The scheme should protect against recipients attempting to redeem the same e-donation more than once and from stores attempting to deposit an e-donation multiple times. Ideally such double-spending or double-depositing should be prevented, although detection must be possible where prevention is not. Moreover, only the holder should be able to initiate a redemption transaction. Stores must be able to detect attempted double-spending without requiring any online verification from charities.

3.3 Integrity

Integrity ensures that information is not altered by unauthorised participants during storage or transmission, without detection by the scheme participants. E-donation data may be manipulated to attack the system. For example, a dishonest recipient may try to change an e-donation to extend its validity period or increase its value. Alternatively, an operator of a false or manipulated store terminal may interrogate the recipient's card and extract information which can later be used to obtain goods from a genuine store (at the expense of the genuine recipient).

To combat the above threats, it must not be possible to successfully fake or modify an e-donation.

4 Anonymous Public Keys

The proposed scheme uses anonymous public keys (APKs), i.e. certified public keys where the owner is anonymous to the verifier [5]. These public keys can be used in the same way as true public keys. Although the PS knows the user's identity, the PS cannot eavesdrop on the user's encrypted communication or forge a digital signature of the user.

We now sketch one method of implementing APKs (as described by Oishi et al. [5]), which applies to public keys for a discrete logarithm based signature scheme.

1. A user X registers his identity id_X and public key P_X with the PS, where P_X is generated using a discrete logarithm base g.
2. First, the PS convert the pair (g,P_X) to another pair (g',P'_X). These two pairs, however, are associated with the same private key S_X.
3. Next, the PS generates an anonymous public key certificate that consists of the converted public key P'_X, additional information (e.g. identity of the PS, validity period, etc.) and a signature on them generated by the PS.
4. Finally, the PS sends the anonymous public key certificate $\mathrm{Cert}_{P'_X}$ to X.

5 Proposed Scheme

We now present a secure electronic payment scheme for charity donations.

5.1 System set up

When initially establishing the system, the PS must decide on a number of fundamental system parameters, which must be reliably communicated to all parties within the system. These include selecting:

- A signature algorithm, where $s_{S_X}(M)$ denotes the signature on message M using the private signing key of entity X,

- A Message Authentication Code (MAC) algorithm, where $\mathrm{MAC}_K(M)$ denotes the MAC computed on message M using secret key K,
- A scheme for generating Anonymous Public Keys, and
- An anonymous electronic cash system with revocable anonymity that the PS must operate; an example of such a system is given in [4].

The CA must also generate its own signature key pair, used for generating public key certificates, where the CA-generated certificate for public key P_X is written as Cert_{P_X}.

Prior to use of the system every participating charity and store must generate and securely store their own secret MAC keys, denoted KC and KS respectively. Additionally, the participating organisations (charities, stores, and the PS) must register with the CA operating the system. Registration will involve the organisation (X say):

- Generating a signature key pair, with private key S_X and public key P_X,
- Obtaining a certificate Cert_{P_X} for P_X from the CA, and
- Obtaining a reliable copy of the public certificate verification key of the CA.

Each donor must be issued with a smart card by a charity, where smart card personalisation and issue involve the following steps.

1. The recipient card must be equipped with a signature key pair.
2. During smart card personalisation, the charity stores in the card a copy of the CA public key, the card expiry date, the charity public key certificate Cert_{P_C}, the card public key certificate Cert_{P_R} signed by the charity, and the recipient unique identifier id_R.
3. To prevent misuse of stolen or borrowed cards, we assume that PIN entry by the authorised cardholder is required to use a recipient card.

The proposed scheme is composed of five phases: the *Initialization phase*, in which the store provides the charity with e-donation tokens that can be redeemed from the store during a specified interval of time, the *Anonymity phase*, in which the donor obtains an anonymous identity and an electronic coin from the PS, the *E-donation definition phase* wherein the donor selects an e-donation token to donate and pays for it, the *Donation phase* during which the charity loads the e-donation into a recipient smart card for redemption from a participating store, and the *Redemption phase* wherein the recipient pays an e-donation to a participating store in exchange for the described goods. In the scheme description, $X||Y$ denotes the concatenation of data items X and Y.

5.2 Initialization phase

The store provides the charity with a token for generating e-donations that can be redeemed from the store during a specified interval of time. I.e.

$$token = s\_data||\mathrm{MAC}_{KS}(s\_data)$$

where

$$s\_data = Item||Value||Expiry||id_S||id_C$$

and where $Item$ specifies the goods, $Value$ denotes the cost of the goods, $Expiry$ indicates the expiry date of the token, and id_S and id_C are identifiers for the store and the charity respectively.

The MAC protects the integrity of the token. The charity publishes the received e-donation tokens on its web site. This gives the donors choices for the donations.

5.3 Anonymity phase

This phase involves the donor and the PS. A donor must first obtain an APK certificate from the PS. Donors then withdraw electronic coins from the PS which can only be used to purchase e-donations from a participating charity. The electronic cash system is operated by the PS which acts as a bank to donors and charities. The charity scheme requires the e-cash system to possess three main functions (typically involving special purpose exchanges of messages):

- Withdraw(val): A donor withdraws a coin c of value val from the PS.
- Payment(c): A donor pays a charity a coin c to make an e-donation.
- Deposit(c'): A charity deposits a spent coin c' with the PS which credits the charity account with the amount of val.

We now describe the anonymity phase:

1. If the donor D does not have an APK certificate from a previous donation, the donor generates a signature key pair (with private key S_D).
2. The donor visits the PS web site and submits: the donor identity id_D, the amount val to be donated, payment information (e.g. an account number), and the public key to be anonymously certified.
3. After collection of the payment from the donor using the specified payment information, the PS uses the provided donor public key to create the anonymised donor public key P_D, and generates an APK certificate Cert_{P_D} for P_D.
4. The donor uses the PS withdraw function to obtain a coin c of value val. The donor can use this coin to make an anonymous e-donation to a participating charity.

5.4 E-donation definition phase

This phase starts when a donor visits a charity web site and decides to donate through this charity. After browsing through the available e-donation tokens provided by participating stores, he selects the token that satisfy his requirements for value, donation type (e.g. food or clothing), validity period, and location where the e-donation will be spent. Then the donor sends an e-donation request to the charity. To construct the request, the donor signs a message that contains the selected charity token and a time stamp T to ensure message freshness. The donor send the message, along with his APK certificate Cert_{P_D}, to the charity.

$Donor \longrightarrow Charity : s_{S_D}(\,token||T)||Cert_{P_D}$

After successful verification of the donor certificate, the signature on the message, and the expiry date within *token*, the charity creates an entry *c_data* in a donation requests database. We assume that the charity keeps a database of all donation requests received and awaiting use for generation of an e-donation. I.e. it generates

$$c\_data = token||Serial\_number||Creation\_time$$

where *Serial_number* is a number that uniquely identifies this entry and *Creation_time* indicates the date/time that the entry was created by the charity.

On generating the entry, the charity signs and sends a response message to the donor. The message contains a signed copy of the generated entry along with the charity certificate Cert_{P_C}

$Charity \longrightarrow Donor :\ c\_data||s_{S_C}(\,c\_data)||Cert_{P_C}$

On receiving the above message, the donor verifies the signature and that the entry was generated according to the donor requirements. If successful the donor and the charity engage in an electronic cash payment protocol that allows the donor to pay the coin c to the charity for the generated entry.

$Donor \longleftrightarrow Charity$: Payment (c)

Upon receiving the payment from the donor, the charity interacts with the PS in an electronic cash deposit protocol to deposit the received coin c'.

$Charity \longleftrightarrow PS$: Deposit (c')

If successful the charity adds the generated entry *c_data* to its database of donation requests. The donor must trust the charity to spend the donated coin in the way requested.

5.5 Donation phase

In this phase, the recipient smart card and the charity terminal engage in an authentication protocol during which the recipient smart card receives e-donations. This protocol conforms to the mutual entity authentication mechanism specified in clause 5.2.2 of ISO/IEC 9798-3 [1].

This phase begins when the recipient presents his card to receive e-donations. First, the charity terminal reads the recipient's identity id_R and the recipient card public key certificate Cert_{P_R} from the card. Then, the charity generates a random number $r2$ and sends it to the recipient card along with its unique identifier id_C.

1. $Charity \longrightarrow Recipient: \ r2\,||id_C$

After receiving the message in step 1, the recipient card generates a random number $r3$ as a challenge to the charity. It then creates a signed message that contains $r3$, the charity identity id_C and the received random number $r2$. The recipient card sends the generated signature to the charity terminal along with $r3$.

2. $Recipient \longrightarrow Charity: \ r3||s_{S_R}(r2\,||\,r3||id_C)$

After receiving the message in step 2, the charity terminal uses the recipient card public key certificate Cert_{P_R} to verify the received signature. If the verification fails, the process is terminated and the card is rejected. Otherwise, the charity terminal generates a response message that contains an $e-donation$ and sends it to the recipient card.

When a charity chooses to issue an $e-donation$ to a recipient, it retrieves an entry c_data from the donation requests database and adds $Issuance\_time$, the date/time this $e-donation$ is issued, and the recipient unique identity id_R to that entry. Then, using its secret key KC, the charity terminal computes and adds $\mathrm{MAC}_{KC}(c\_data||Issuance\_time||id_R))$ to the retrieved entry. Thus,

$$e{-}donation = c\_data||Issuance\_time||id_R||\mathrm{MAC}_{KC}(c\_data||Issuance\_time||id_R)$$

The charity terminal now creates a signed message that contains the random numbers received in step 2, the recipient identifier id_R, and the $e-donation$. The charity sends the $e-donation$ and the generated signature to the recipient card.

3. $Charity \longrightarrow Recipient: \ e-donation||s_{S_C}(\,r3||\,r2||id_R||\,e-donation)$

Upon receiving the message in step 3, the recipient card uses the stored charity public key certificate to verify the charity signature. If the check fails, the process is terminated and the card does not accept any information from the terminal. Otherwise the card updates its stored list of e-donations. We assume that the charity keeps a database of all e-donations issued during a specific period. The charity also deletes the c_data used in the $e-donation$ generation from the donation requests database, and adds an entry to the e-donations database.

5.6 Redemption phase

In this phase, the recipient card and the store terminal engage in an authentication protocol during which the store terminal retrieves e-donations stored in the recipient card in exchange for goods. The recipient must trust the store terminal not to remove e-donations not authorised by the recipient.

First, the store terminal reads the recipient unique identity id_R, the card expiry date, the charity public key certificate, the recipient card public key certificate and the list of e-donations. If the card has not expired, then the store terminal verifies the recipient card public key certificate using the charity public key certificate, which in turn can be verified using the CA's public key known to the store terminal. If successful, then the store terminal displays to the recipient a list of unredeemed e-donations, from which the recipient selects the one that is to be redeemed. Moreover, the store terminal asks the recipient card for a challenge.

The recipient card responds by generating a random number $r4$ and sends it to the store terminal.

1. $Recipient \longrightarrow Store:\ r4$

After receiving the message in step 1, the store terminal generates a random number $r5$ as a challenge to the recipient card. It then creates a signed message that contains $r5$, the store identity id_S and the received random number $r4$. The store terminal sends the generated signature to the recipient card along with $r5$, id_S and the store public key certificate Cert_{P_S} .

2. $Store \longrightarrow Recipient:\ r5||id_S||s_{S_S}(\ r5||\ id_S||r4)||Cert_{P_S}$

When the recipient card receives the message in step 2, it uses the stored CA public key to verify the store's public key certificate. If successful the card uses it to verify the received signature. If the signature verifies successfully, the recipient card responds with a message that contains the selected unspent e-donation and a signature computed over the concatenation of that $e-donation$, $r5$, and the identities of both the recipient and the store.

3. $Recipient \longrightarrow Store:\ e-donation||s_{S_R}(e-donation||r5||id_R||id_S)$

Upon receipt of the message in step 3, the store verifies the recipient card signature. If the signature verifies successfully, then the store uses its secret key KS to recompute $\mathrm{MAC}_{KS}(s\_data)$ and then checks the result against the received $e-donation$. If the check succeeds then it accepts the $e-donation$ as valid and proceeds with providing the goods specified in the $e-donation$ to the recipient. Moreover, the recipient card marks the $e-donation$ used in message 3 as spent.

To help protect the card against fraud by the store, the recipient card logs message 3 for later settlement by the charity.

Similarly, protection of the store against the recipient is provided by exchanging the goods stated in the $e-donation$ for the message in step 3. The store later uses message 3 to collect the corresponding monetary amount from the charity.

Typically, the transactions would be sent in a batch, signed by the store so that the charity can verify the integrity and authenticity of the transaction batch.

6 Security analysis

In this section, we examine to what extent the generic security requirements outlined in section 3 are met by our scheme.

6.1 Donor Anonymity

The anonymity of the donor is protected from the charity using the APK certificate, which allows a donation to be made to a charity without revealing the donor's real identity. Although the donor is not anonymous to the PS, since the donor makes a payment in exchange for an APK certificate and an electronic cash coin, it is not possible for the PS to know what donation a donor makes because the coin used to make the donation is anonymous. The PS would need to deanonymize the coin deposited by a charity to reveal the identity of the withdrawer.

6.2 Double-spending

Protection from e-donation double spending is provided by means of smart cards. Our e-donation scheme is an offline system, i.e. the store does not need to contact the charity for every redemption performed by a recipient. Instead, the scheme relies on a tamper-resistant recipient card that uses cryptographic means to recognize when it is communicating with a member of the scheme (e.g. charity or store). The charity and the recipient trust the recipient card to update its list of e-donations every time it is involved in a donation or redemption transaction with a member of the scheme. Moreover, since the recipient card is tamper-resistant, an attacker cannot modify the card contents without permanently damaging the card. Therefore, the recipient cannot benefit more than once from the same e-donation. The disadvantages of using the smart card approach is that no card is completely tamper resistant, and the cost associated with setting up the scheme may be significant.

On the other hand, the charity maintains a database of all e-donations which have been issued. The charity uses the redeemed e-donations received from stores and recipient cards logs to detect and punish double spending afterwards.

Typically, an e-donation would have a limited validity (days) to limit the problems of forgery, and to limit the size of the e-donation database. This database will be large, but not infeasibly so. There will need to be one database record per generated e-donation.

6.3 Integrity

Integrity protection for the e-donation data is accomplished using message authentication codes and digital signatures. Calculating a message authentication code over parts of the messages exchanged using a key known only to the authorised parties provides evidence to the verifier that the message content has not been altered or destroyed, accidentally or with malicious intent, since it was created.

For example, if an attacker decided to change the *Item* field found in the *s_data* part of $e - donation$ to his benefit, the attacker would need to modify $\mathrm{MAC}_{KS}(s\_data)$ to reflect the new value of the *Item* field. However, our scheme assumes that no one other than the store who computed the original $\mathrm{MAC}_{KS}(s\_data)$ knows the key KS. Moreover, we assume that the MAC function used is secure. The use of a MAC thus prevents such an attack.

On the other hand, theft of e-donations paid to a store is prevented by making such e-donations depositable only by that store. This is done by including the identity of the store in the signature $s_{S_R}(e - donation||r5||id_R||id_S)$, which is created by the recipient card in step 3 of the *Redemption phase*.

7 Conclusion

In this paper we have proposed a scheme to make and distribute charitable donations electronically using the Internet and smart cards. We described the scheme in detail, and explained how it meets the identified security requirements. In the future, a prototype implementation of the scheme will be built using a Java servelet and Java Card technology. The purpose of the prototype will be to examine the efficiency of a possible practical deployment of the scheme.

It would be interesting to investigate how the proposed scheme could be modified to allow the recipient to receive and redeem e-donations using a mobile phone instead of a smart card.

References

1. ISO/IEC 9798-3. *Information technology — Security techniques — Entity authentication mechanisms — Part 3: Mechanisms using asymmetric signature techniques*. International Organization for Standardization, Geneva, Switzerland, 1998.
2. D. Chaum. Blind signatures for untraceable payments. In D. Chaum, R.L. Rivest, and A.T. Sherman, editors, *Advances in Cryptology—CRYPTO '82*, pages 199–203. Plenum Press, August 1983.
3. Smith Craver, Mathews and Company. Socially engaged internet users: Prospects for online philanthropy and activism, 1999. available at http://www.craveronline.com.
4. D. Kugler and H. Vogt. Fair tracing without trustees. In Paul Syverson, editor, *Proceedings of Financial Cryptology 2001*, number 2339 in Lecture Notes in Computer Science, pages 136–148, Springer-Verlag, Berlin, 2001.
5. K. Oishi, M. Mambo, and E. Okamoto. Anonymous public key certificates and their applications. *IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Sciences*, E81-A(1):56–64, January 1998.
6. S. von Solms and D. Naccache. On blind signatures and perfect crimes. *Computers & Security*, 11(6):581–583, 1992.