NON-REPUDIATION WITH MANDATORY PROOF OF RECEIPT

Tom Coffey and Puneet Saidha
University of Limerick
Ireland

ABSTRACT

Non-repudiation allows an exchange of data between two principals in such a manner that the principals cannot subsequently deny their participation in the exchange. Current non-repudiation schemes, while providing a mandatory *proof of origin* service, generally provide only discretionary *proof of receipt* since it is difficult to enforce the return of the *proof of receipt* by the recipient.

In this paper a new scheme for achieving mandatory mutual non-repudiation is proposed, encompassing both mandatory *proof of origin* and mandatory *proof of receipt*. The fundamental feature of the scheme is that the proofs of origin and receipt are not exchanged until both principals have submitted their digitally signed evidence to a trusted third party intermediary. This ensures that if the non-repudiation protocol is not completed, neither principal can gain from the exchange. An added advantage is that the process of dispute arbitration is considerably simplified since a small number of rules are required to decide whether an alleged data exchange took place.

Keywords: Non-Repudiation, Digital Signatures, Proof of Origin, Proof of Receipt, Dispute Arbitration, Security Protocols, Public-Key Cryptography.

1. INTRODUCTION

Repudiation is the denial by one of the entities involved in a communication of having participated in all or part of the communication [ISO89]. Non-repudiation is concerned with preventing such a denial. With sender non-repudiation, the originator of a data exchange is provided with a *proof of receipt* (POR) which proves that the recipient received the data. Receiver non-repudiation provides the recipient with a *proof of origin* (POO) which proves that the originator sent the data. The proofs of origin and receipt constitute non-repudiation evidence information. Principals can exchange evidence information, either through direct peer-to-peer communication or indirectly via a third-party intermediary (see figure 1).

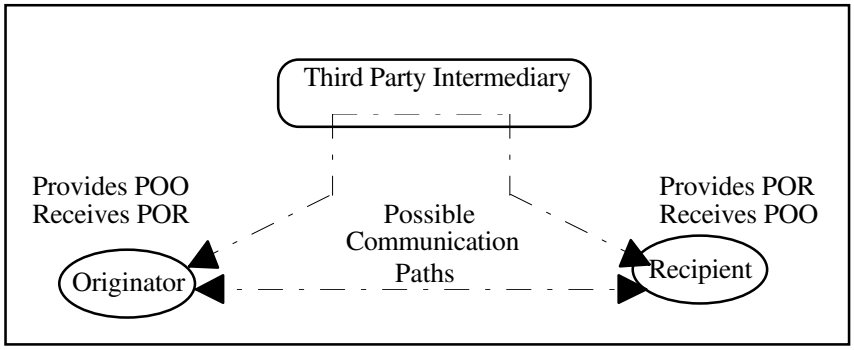

Figure 1: Non-Repudiation Service

The correct generation of evidence information is crucial to non-repudiation. The *proof of origin* must associate the identity of the originator with the data exchanged in such a manner that the originator cannot deny this association. Likewise, the identity of the recipient is associated with the *proof of receipt*. The evidence must be undeniable and unforgeable. These properties are achieved through the use of digital signatures.

A non-repudiation service must provide an arbitration framework for addressing disputes. If a dispute arises, it may be possible for the disputing principals to resolve it themselves by exchanging and examining the evidence information. If this does not suffice, then an agreed arbitrator, which is trusted by both principals, is called upon to reach a settlement. The entities involved in the exchange present evidence to this arbitrator who uses a set of well-defined rules to decide, based on the evidence submitted, whether or not an exchange took place.

The remainder of this section briefly presents the approach of existing non-repudiation schemes. In section 2, we discuss the use of digital signatures, which are used to generate non-repudiation evidence information. In section 3, we outline the key feature of our method. The third-party services required for the operation of our scheme are presented in section 4. In section 5, we give step-by-step details of our non-repudiation protocol. The dispute arbitration process is discussed in section 6 and the decision-making rules are given. Finally, our conclusions are presented in section 7.

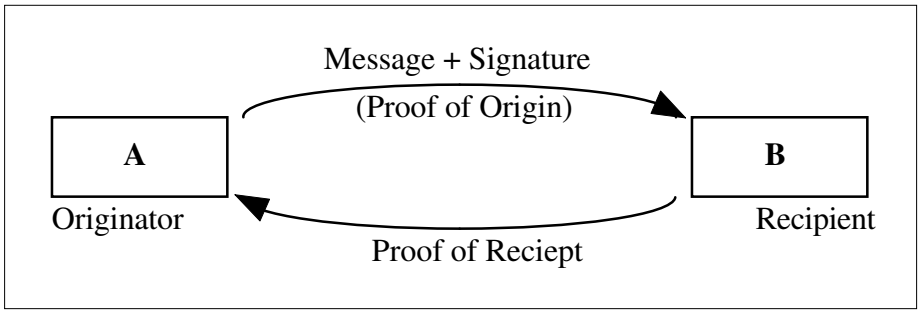

Figure 2 : Simple Non-Repudiation Scheme

1.1 General Approach to the Non-Repudiation Problem

Non-repudiation is sometimes implemented using a simple peer-to-peer protocol whereby the originator sends the message along with his signature, thus providing the recipient with the *proof of origin* for the message and the recipient, in turn, returns a signed *proof of receipt* to the originator (see figure 2). Examples of techniques based on this method can be found in [Barb91] and [Herd95].

Generally, the difficulty with such non-repudiation schemes is in enforcing mandatory evidence exchanges. From figure 2 above, it is clear that the recipient will obtain the *proof of origin* so that the sender non-repudiation is a mandatory service. However, the *proof of receipt* service is more difficult to implement [KBN88] and is generally discretionary in nature.

2. DIGITAL SIGNATURES

A non-repudiation service must undeniably associate the identities of the communicating principals with the non-repudiation evidence information. This is achieved using digital signatures [DH76]. A digital signature is formed using the secret key of the signing entity. If this secret key has not been compromised, then the signature is unforgeable and undeniable. To verify a digital signature, the public key of the signing entity is used. In the X.509 recommendation [CCITT88], a digital signature scheme is defined which also provides for data integrity validation. Figure 3 illustrates the generation and validation of the digital signature DSG_A of entity A for message M.

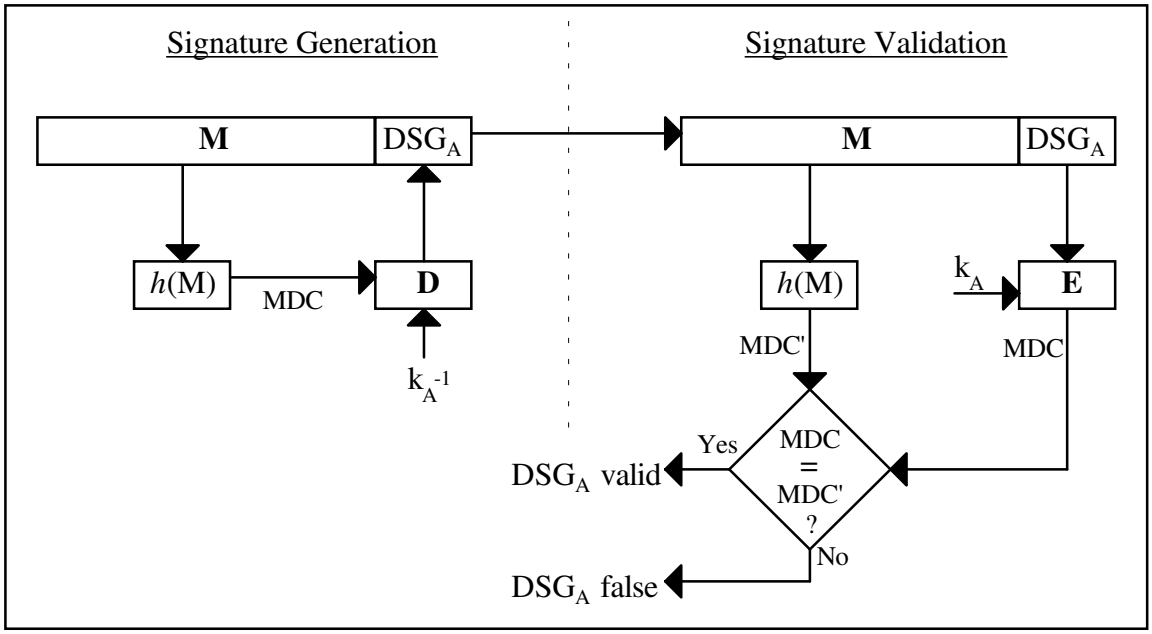

Figure 3: Digital Signature Generation and Validation

Signature generation is as follows:

i. A Modification Detection Code (MDC) is generated for M using a one-way hashing function *h*.

$$MDC = h(M)$$

The MDC is a short data item of standard length which is a function of the complete message so that any difference, no matter how small, between two messages will cause different checksums to be generated.

ii. The signature DSG_A is obtained by decrypting this MDC with the secret key k_A^{-1} of the signer.

$$DSG_A = D_A(MDC)$$

iii. The signed message S then consists of the plaintext message M with the signature DSG_A appended to it.

$$S = M + DSG_A$$

During signature validation, the original MDC is recovered by encrypting DSG_A with the public key k_A. A new MDC' is generated by hashing M. Comparing MDC and MDC' reveals whether or not the signature is valid. It can be seen that this scheme provides for data integrity. If M is altered in any way, then the MDC' generated during signature validation will be different from the original MDC. This indicates that the signed message should be rejected.

2.1 Reliability of Digital Signatures

For the digital signature mechanism to function reliably, certain assurances need to be provided in relation to the goodness of the public/secret key pairs.

i. To verify the digital signature of an entity A, its public key k_A is required. If false signatures are to be detected, then it must be possible to know with absolute certainty that k_A does, in fact, belong to the entity A. Certificates [CCITT88] provide such assurance. A certificate unforgeably associates the name of a principal with its public key and is digitally signed by the trusted certification authority of that principal, thus ensuring that the public key contained therein is secure and correct [WC92].

ii. If a secret key has been compromised, then the corresponding public key is no longer deemed to be good. In such a case, the certification authority will revoke the certificate containing that key [GGKL89]. A digital signature formed using a compromised key is not valid and therefore, a signature verifier must be sure that the public key to be used in the verification has not been revoked.

iii. A certificate has a limited validity period. A digital signature is only valid if the secret key used in its generation is in date. However, a dispute can arise in relation to a non-repudiable exchange after the keys used have expired. As Linn points out, if long-term non-repudiation is to be achieved, it may be necessary to make use of expired certificates during arbitration [Linn91]. Therefore, the time of signing must be known for a piece of evidence information. Time-stamps are used for this purpose (see section 4.2).

To ensure that only good public keys are used, the appropriate certificates should be obtained from the certification authorities immediately prior to the execution of the non-repudiation protocol. This provides a signature verifier with the most up-to-date revocation status of a certificate. A certification authority is trusted by its principals not to distribute revoked or invalid certificates.

3. OUR NON-REPUDIATION SCHEME

We propose a non-repudiation scheme which provides for mandatory *proof of origin* and mandatory *proof of receipt* through the use of a trusted third party intermediary, called the Non-Repudiation Server (NRS). The basis of this scheme is that the proofs of origin and receipt are not exchanged until both principals have submitted their signed evidence to the NRS. Figure 4 illustrates the two phases involved. In phase 1 of the scheme, the NRS gathers the evidence information (proofs of origin and receipt) in such a way that the recipient cannot learn the *proof*

of origin and the originator cannot learn the *proof of receipt*. When the NRS is in possession of both pieces of evidence, it then distributes these to the communicating parties in phase 2. Therefore, it is mandatory for both principals to provide evidence to the NRS. If this is not done, then neither principal can gain from the message transfer. The details of the dispute arbitration procedure for our scheme can be found in section 6.

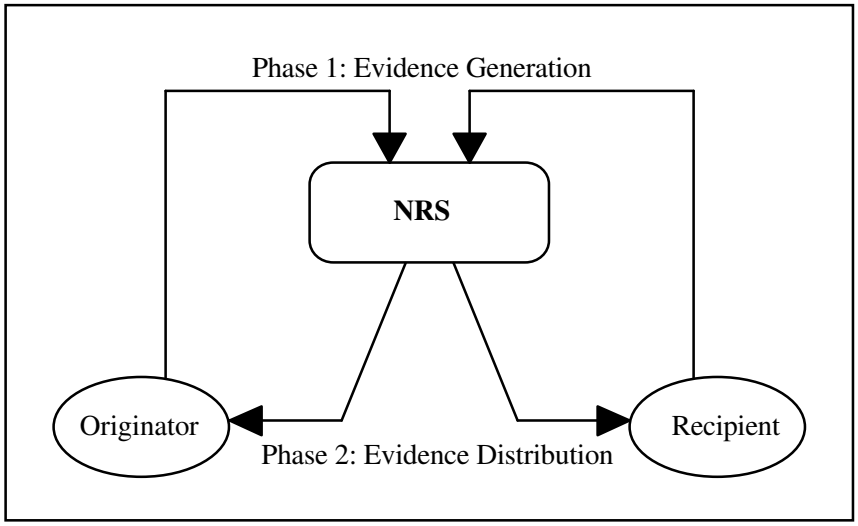

Figure 4: Proposed Non-Repudiation Scheme

The main benefit of our scheme is that it allows for easier enforcement of the *proof of receipt* service. Both the originator and the recipient must fulfil their roles before any useful information is exchanged between them. In addition, our scheme allows the use of very simple dispute arbitration rules.

4. TRUSTED THIRD PARTY REQUIREMENTS

Our non-repudiation service requires that all communication between the originator and recipient takes place through a trusted third party intermediary and that all digitally signed evidence is accompanied by reliable and trustworthy time-stamps. These requirements are satisfied through the provision of a non-repudiation server (NRS) and a time-stamping authority (TSA). Both of these are trusted entities. Two principals exchanging data may not necessarily trust each other, but they must both trust the jurisdiction and reliability of the non-repudiation server and the time-stamping authority. In a hierarchical network environment, the establishment of such trust may require the use of a trust-path mechanism [WC92], whereby an entity is assumed to trust its parent entity, which in turn trusts its parent, and so on. A trust-path is thus formed from the originator and recipient to a common authority which is then trusted by both.

4.1 Trusted Third Party Non-Repudiation Server

The proposed non-repudiation scheme depends on a non-repudiation server to co-ordinate the exchange of the required pieces of proof information. The following points can be noted in relation to the NRS:

i. The NRS is independent of the communicating principals and is trusted by them.

ii. The NRS will not distribute proof information to either one of the communicating principals unless it possesses the appropriate proof information for distribution to the other principal.

iii. The NRS receives the *proof of origin* directly from the originator and co-operates with the recipient to generate the *proof of receipt*.

iv. Once the NRS has received all required pieces of proof information for both communicating principals, then it will not renege in its duty to distribute the appropriate information to each principal. Therefore, if the NRS has possession of the proof information, it is assumed that the communicating principals can readily obtain this information.

The role of this NRS is critical to the operation of the non-repudiation service and we recommend that some additional provisions be made outside the scope of the protocol specification to ensure its feasibility. Contractual agreements should be made between the protocol users so that they are legally bound to accept the authority of the NRS. With such agreements in place it is assumed that, once the NRS has obtained all the necessary evidence, users are assumed to be capable of receiving this evidence from the NRS. Such agreements prevent users from denying receipt of proof information from the NRS itself. In this way, the NRS can be seen to act as an agent for each of the communicating principals. The possible structure and content of such contractual agreements are a question of law and are beyond the scope of this paper. A second provision is to use a statutory authorization to empower the NRS and to regulate its role and responsibility. This would mean that the NRS is legally bound to fulfil its duty honestly.

4.2 Trusted Third Party Time-Stamping Authority

One of the features of X.509 public key certificates is that they have limited validity periods. During a non-repudiation protocol execution, no principal should make use of a certificate which has expired. However, in the case of a dispute occurring after the validity period of a certificate, it may be necessary to make use of the expired certificate for signature verification during arbitration. Therefore, the time of signing needs to be known for each digitally signed piece of evidence, to determine whether the corresponding public key was valid at that time.

The time of signing is recorded by appending a time-stamp to the evidence information. However, some care is needed here. If the communicating principals are to apply their own time-stamps, then there must be some guarantee that their local time references are accurate and tamper-proof. For a large distributed system, it can be difficult to provide such a guarantee. It is preferable to make use of a third party which is trusted by both communicating parties to provide reliable time-stamps. If a message M is to be stamped, it is transmitted to the time-stamping authority which appends its own identifier TSA and the time-stamp and then signs the entire message. The time-stamping authority provides a generic service and is not concerned with the contents of the message being stamped. The operation is illustrated in figure 5.

Since, when using such a technique, there will be short delay between the time of signature generation and the time at which the time-stamp is applied, it must be the responsibility of the requesting principal to ensure that its certificate does not expire during the time-stamping process.

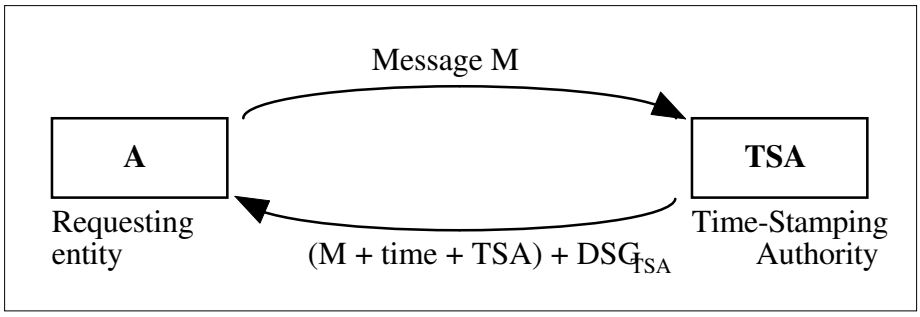

Figure 5 : A Trusted Third Party Time-Stamping Service

5. A PROTOCOL TO IMPLEMENT OUR NON-REPUDIATION SCHEME

This protocol enables two principals to exchange non-repudiation proof information, incorporating mandatory *proof of origin* and mandatory *proof of receipt*.

5.1 Notation

In the protocol specification given below, the following notation is employed:

The two pieces of evidence information exchanged during a non-repudiable exchange are the *Proof of Origin* (POO) and the *Proof of Receipt* (POR). Their structures are as follows:

$$POO = \left[\left(\left[type1,\ A,\ B,\ msg\right]dsgA\right),\ TSA,\ ts1\right]dsgTSA$$

$$POR = \left[\left(\left[type2,\ B,\ A,\ h(POO)\right]dsgB\right),\ TSA,\ ts2\right]dsgTSA$$

where,
type1 : field which indicates that this structure is intended as a *proof of origin*
type2 : field which indicates that this structure is intended as a *proof of receipt*
A : the distinguishing identifier of the originator
B : the distinguishing identifier of the recipient
TSA : the distinguishing identifier of the time-stamping authority
msg : the message to be exchanged
h(M) : a one-way hashing function applied to message M
[M]dsgX : the digital signature of entity X appended to the message M
ts1, ts2 : the time-stamps
{M1,M2} : the concatenation of messages M1 and M2 without any change to their contents

The remaining notation used in the protocol specification is as follows:

k_X : public key of entity X
k_X^{-1} : secret key of entity X
{M}k : encryption/decryption of message M using the key k
n1_NRS, n2_NRS : random nonces generated by the NRS
S → R : {M} : This means that the entity S sends message M to entity R.

5.2 Protocol Steps

The diagram of figure 6 illustrates the interactions between the communicating principals. The numbers on the transition arcs refer to the protocol steps described below.

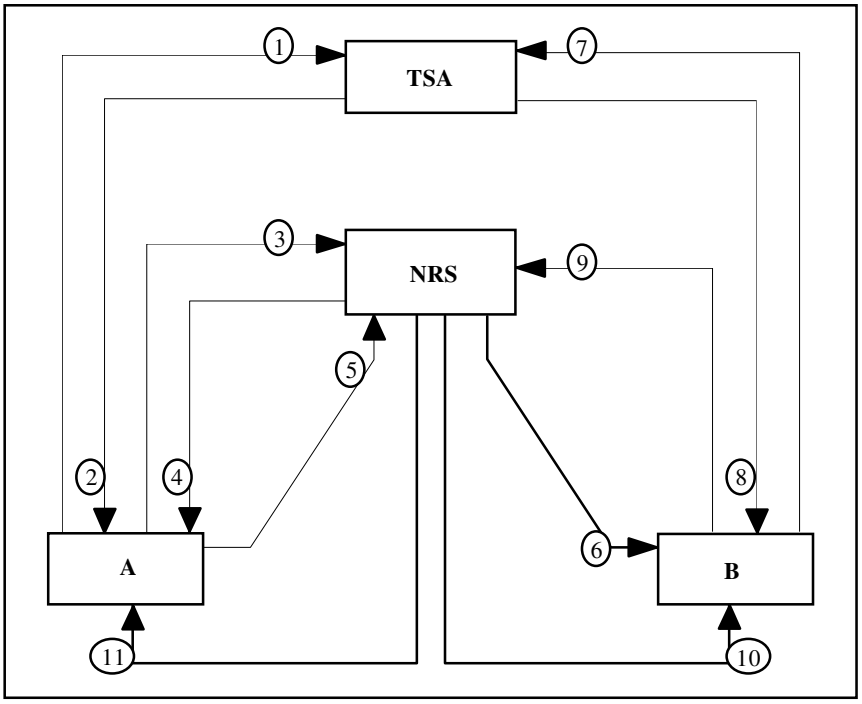

Figure 6 : The Non-Repudiation Protocol

Step 1: **A → TSA : { p_poo }k_{TSA}**
Before entering into any communication with the NRS, originator A must first generate a *proof of origin* which includes a valid time-stamp. To this end, A first constructs a *partial proof of origin* p_poo, which is forwarded to the TSA to have the time stamp appended.
p_poo = [type1, A, B, msg]dsgA

Step 2: **TSA → A : { POO }k_A**
The TSA adds a time-stamp to the received p_poo to form a complete POO.
POO = [p_poo, TSA, ts1]dsgTSA
The POO is sent to A who can verify that the time-stamp is valid.

Step 3: **A → NRS : { "N_R_req" }**

The originator initiates communication with the NRS by sending a message requesting a non-repudiable data transfer.

Step 4: **NRS → A : { n1_NRS }k_A**

The NRS sends a challenge nonce n1_NRS to A. Since A will require the use of k_A^{-1} to recover this nonce, only the authentic A will be able to discover its value.

Step 5: **A → NRS : { [n1_NRS, POO, p_por]dsgA }k_{NRS}**

Originator A formulates a message incorporating the challenge response n1_NRS which guarantees to the NRS that the message is not a replay, the complete *proof of origin* and a *partial proof of receipt* p_por which is defined as follows:

p_por = {type2, B, A, *h*(POO)}

While it would be possible for the NRS itself to construct this p_por from the received POO, the originator provides it here so as to minimise computation on the part of the NRS.

Step 6: **NRS → B : { [n2_NRS, p_por]dsgNRS }k_B**

The NRS initiates the *proof of receipt* generation by forwarding the p_por along with the challenge nonce to the recipient.

Step 7: **B → TSA : { s_p_por }k_{TSA}**

B signs the received p_por with his secret key k_B^{-1} to form the *signed partial proof of receipt* s_p_por as follows:

s_p_por = [type2, B, A, *h*(POO)]dsgB

This s_p_por is then sent to the TSA to have a time-stamp appended.

Step 8: **TSA → B : { POR }k_B**

The TSA appends a time-stamp to the received data, thus forming a complete POR.

POR = [s_p_por, TSA, ts2]dsgTSA

This is then returned to B who can verify that the time-stamp is valid.

Step 9: **B → NRS : { [n2_NRS, POR]dsgB }k_{NRS}**

B now returns the complete POR to the NRS along with the challenge nonce n2_NRS. The NRS can verify that the POR received is valid and is not a replay.

Step 10: **NRS → B : { POO }k_B**

The NRS stores a copy of the POR and POO for later use. The POO is sent to the recipient who can examine the data contained therein.

Step 11: **NRS → A : { POR }k_A**

The NRS sends the POR to the originator.

6. HANDLING DISPUTES IN OUR NON-REPUDIATION SCHEME

If a dispute arises in relation to a non-repudiable data exchange, an agreed arbitrator which is trusted by both principals may be called upon to resolve it. The entities involved in the exchange present evidence to this arbitrator who makes use of arbitration rules to reach a decision regarding the exchange. Three entities may submit evidence - the NRS, the originator and the recipient. The arbitrator's decision-making rules must allow for the submission of any combination of evidence by these three entities. In reaching a decision, the arbitrator will deem that a data exchange did not take place in the absence of sufficient evidence to prove otherwise.

The decision-making rules are as follows:

i. **If** originator knows POR, **then** this is proof that the recipient received the data, i.e. the data exchange did take place
ii. **If** recipient knows POO, **then** this is proof that the originator did send the data which the recipient now possesses, i.e. the data exchange did take place
iii. **If** NRS knows POR, **then** this is proof that the protocol at least successfully completed step 9, by which stage, the data exchange is deemed to have taken place
iv. **If** NRS knows POO, **then** this is proof that the protocol at least successfully completed step 5, by which stage, the data exchange is not deemed to have taken place

Using these four rules, it is possible to reach a decision regarding any claimed non-repudiable exchange. For instance, if the originator submits a POR, then regardless of whether any of the other entities submit evidence, the arbitrator knows that the exchange took place. Table 1 shows the different possibilities of evidence submission and the decisions which follow from them. The symbol 'X' indicates a "don't care" state. The first three rows of this table are directly obtained from rules i, ii and iii above. For each of these cases, evidence submitted by just one of the participating parties is sufficient to prove that the exchange took place. The last row is based on the fact that the submission of the POO by the NRS does not prove a data exchange (rule iv). Therefore, if no evidence is submitted by the other participants, then the arbitrator must conclude that the data exchange did not take place.

NRS Submits		Originator	Recipient	Data Exchange
POO	POR	Submits POR	Submits POO	Took Place
X	YES	X	X	YES
X	X	YES	X	YES
X	X	X	YES	YES
X	NO	NO	NO	NO

Table 1: Criteria for deciding Dispute Arbitration Rules

7. CONCLUSIONS

We have proposed a solution for achieving a non-repudiable data transfer service which provides for mandatory *proof of origin* and mandatory *proof of receipt*.

Our service makes use of public-key cryptography and is dependent on a number of assumptions. We believe that all assumptions are justifiable. Perhaps the most crucial feature of the scheme is the heavy dependency on the trust in the non-repudiation server. However, some additional provisions such as contractual agreements between the users or a statutory authorization for the NRS can justify this dependency.

The actual non-repudiable exchange is realised by means of a communication protocol which involves the originator of the data, the NRS and the recipient of the data. We have presented the dispute arbitration rules which apply to this protocol. These rules are based solely on the evidence submitted to the arbitrator by the various parties involved.

One of the features of our technique is that fact that communication between end users is not peer-to-peer but rather, takes place via a centralised third party intermediary. This necessitates the use of additional mechanisms for establishing trust in such an intermediary such as the formation of trust-paths. In addition, the practical application of the non-repudiation service is limited by the legal environment which governs it. In a world-wide communications environment, legal jurisdictions vary and the trust issues associated with non-repudiation become more complex. Therefore, it is envisaged that primary scope of application for the non-repudiation service is within domains which fall under a single legal jurisdiction.

The binding nature of non-repudiation evidence necessitates the use of formal techniques to ensure that the non-repudiation protocol is free from errors or security defects. A formal proof of correctness for our protocol can be found in [CS95].

REFERENCES

[Barb91] Barbut, Jean-Louis, ETEBAC 5: The standard for secure data exchange between banks and their corporate customers. *SECURICOM'91, 9th Worldwide Congress on Computer and Communications Security and Protection*, (March 1991), 199-214.

[CCITT88] CCITT. The directory - authentication framework. *CCITT Rec. X.509*, (1988).

[CS95] Coffey, T. and Saidha, P. A logical verification of a non-repudiation protocol. *Report #67/95*, Department of Electronics & Computer Engineering, University of Limerick, Ireland, (1995).

[DH76] Diffe, W. and Hellman, M. New directions in cryptography. *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, (Nov. 1976), 644-654.

[GGKL89] Gasser, M., Goldstein, A., Kaufman, C. and Lampson, B. The Digital distributed system security architecture, *1989 National Computer Security Conference*, (1989).

[Herd95] Herda, S. Non-repudiation: constituting evidence and proof in digital cooperation, *Computer Standards and Interfaces*, Vol.17, No.1, (January 1995), 69-79.

[ISO89] ISO. Information processing systems - open systems interconnection - basic reference model - part 2: security architecture, *ISO 7498-1*, (1989).

[KBN88] Karp, B.C., Barker, L.K. and Nelson, L.D. The secure data network system, *AT&T Technical Journal*, (May/June 1988), 19-27.

[Linn91] Linn, J. Privacy-enhanced electronic mail: from architecture to implementation, *Information Security*, (1991), 233-243.

[WC92] Wang, W. and Coffey, T. Network security: design of a global secure link, *Proceedings of the International Federation of Information Processing (IFIP) TC11 8th International Conference on Information Security*, Singapore, (1992), 103-113.