COMPUTERS & SECURITY 27 (2008) 309–322

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

An optimistic fair exchange protocol based on signature policies

*Jorge L. Hernandez-Ardieta**, *Ana I. Gonzalez-Tablas*, *Benjamin Ramos Alvarez*

Information and Communication Technology Security Research Group, Department of Computer Science, University Carlos III of Madrid, Av. Universidad 30, 28911 Leganes (Madrid), Spain

ARTICLE INFO

Article history:
Received 12 February 2008
Received in revised form
25 May 2008
Accepted 9 July 2008

Keywords:
Security
E-commerce
Non-repudiation
Fair exchange
Electronic signature
Digital signature
Signature policy
PKI
Standards

ABSTRACT

The growth of the e-commerce has allowed companies and individuals to sell and purchase almost any kind of product and service through the Internet. However, during the purchase transaction there is a moment during which the seller has sensitive information from the buyer, typically his/her credit card information, while the buyer has nothing from the seller. This situation clearly places the buyer at disadvantage and is, together with fear of fraud, one of the reasons of the lack of confidence in e-commerce. For resolving this situation a new fair exchange protocol based on signature policies is presented. A signature policy is a set of rules to create and validate electronic signatures, under which an electronic signature can be determined to be valid in a particular transaction context. Due to the signature policy-based design, the proposed protocol allows the buyer to decide if trust or not in the rules that will manage the transaction, increasing the user's confidence in e-commerce. Security, fairness and timeliness characteristics of the protocol are evaluated. Implementation guidelines are also provided taking into consideration latest security standards.

1. Introduction

The growth of the e-commerce has allowed companies and individuals to sell and purchase almost any kind of product and service through the Internet in a fast, comfortable and effective manner. The main operational modes are B2C (Business to Customer) and B2B (Business to Business). In the former case the buyer is an individual, in the latter is another company. Although the context is different, in both cases the aim is the same: to purchase a product or service (resource).

Such a purchase implies an electronic transaction. Next, an example of the stages needed for a B2C transaction is described:

1. First of all, the buyer selects the resource to buy.
2. Later, the buyer has to send his/her credit card information to the seller.
3. During next stage a payment gateway is used for communicating with buyer and seller's banks, and for carrying out the charge process (VISA, 1997, 2006; EMV, 2007).
4. Finally, the seller notifies the buyer about the transaction result.

Once the transaction is finished, and depending on the purchase conditions and the resource nature, the buyer obtains either the resource itself or an acknowledgement of receipt. As an example for the first case, purchasing stream content may allow the buyer to start receiving the resource as

* *Corresponding author*.
E-mail address: jlopez.ha@gmail.com (J.L. Hernandez-Ardieta).
0167-4048/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2008.07.005

soon as the transaction is successfully completed. In the second one, the acknowledgement of receipt is the only element the buyer has for making a future complaint. This acknowledgement of receipt acts as a proof of the performed electronic transaction. In e-commerce context, this acknowledgement of receipt may be an electronic invoice.

However, possessing certain information does not always imply a contractual or legal commitment. It is possible for the buyer to auto-generate acknowledgements of receipt or even for the seller to charge as many purchases as desired, once buyer's credit card information is known. Thereby a buyer could reject having participated in an electronic transaction or the seller could not send the resource to the buyer if he suspected that a fraudulent operation was carried out.

Evidence is used for resolving this previous problematic situation (Zhou and Gollmann, 1997). Evidence is generated during the transaction, and obliges both buyer and seller to make a certain commitment. Normally, evidence consists of digital signatures (Diffie and Hellman, 1976) of the information exchanged during the transaction. As an example, in Asokan (1998), evidence is used in several e-commerce protocols proposals. In one of these protocols, the buyer generates evidence on the order and bank account information, while the seller does it on the acknowledgement of receipt. Due to the nature of the evidence, the commitment cannot be repudiated. Therefore, the buyer makes a commitment to paying the agreed price for the resource while the seller makes it to the resource delivering. And no one could, in a future dispute, successfully reject having made those commitments.

Nevertheless, the mere evidence generation does not completely resolve the problem. Due to the division of an electronic transaction into several stages, as seen in the example above, the seller could obtain the evidence from the buyer without sending the corresponding one.

For being a complete fair exchange process, evidence must tie down both buyer and seller on an equal footing. By this, none of them could gain an advantage over the other during the protocol execution.

Several solutions have been proposed in the literature to address fair exchange in e-commerce. These protocols are known as fair exchange protocols. Asokan, in his thesis (Asokan, 1998), offers a deep research on fairness and non-repudiation in e-commerce, reviewing the properties of these protocols and focusing on the design of a generic payment service. In Ray and Ray (2002), several fair exchange protocols are analysed, even from the early gradual exchange protocols. On the other hand, in Bao et al. (1998), the authors propose a new cryptographic primitive called CEMBS (Certificate of Encrypted Message Being a Signature), and from which different fair exchange protocols are built. Conditional digital signatures are proposed in Lee and Kim (2002) as the key element of the fair exchange protocol design. Other authors also use conditional signatures' concept to build protocols for revoking digital signatures in cases where the signer has used a malicious terminal, but out of the context of fair exchange and non-repudiation protocols (Berta et al., 2004a,b, 2005).

The design of fair exchange protocols differs a bit from those known as fair non-repudiation protocols (Coffey and Saidha, 1996; Kremer et al., 2002; Zhou and Gollmann, 1996a,b; Yang et al., 2005), where the exchanged information is, in fact, the non-repudiation evidence. While in a fair exchange protocol both buyer and seller know the items to be exchanged before executing the protocol (e.g. e-commerce scenario), in a fair non-repudiation protocol the recipient of a message does not expect a particular message, knowing it only at the end of the protocol.

However, both fair exchange and non-repudiation protocols share a common aspect: the existence of an entity trusted by both players and that participates during the protocol for assuring the fairness and timeliness. This entity is called Trusted Third Party (TTP), and depending on its degree of involvement during the protocol execution it is considered inline, online or offline – from higher to lower degree of involvement. If the TTP is offline, it only participates in case of player's misbehaviour, improving the performance of the protocol in normal executions. Protocols that incorporate an offline TTP are called optimistic (Asokan et al., 1997; Kremer and Markowitch, 2000; Okada et al., 2008).

This article proposes an optimistic fair exchange protocol which introduces a complete innovative design. The protocol design principle is based on signature policies (ETSI TR 102 041, 2002), a set of rules to create and validate electronic signatures, and under which an electronic signature can be determined to be valid in a particular transaction context. More specifically, the signature policy proposed in this work sets the steps and clauses to be followed by all parties (origin-buyer, receiver-seller, TTP) in an e-commerce transaction in order to assure its fairness, timeliness and security. Due to the signature policy-based design, the proposed protocol allows the buyer to know and evaluate the conditions that will manage the electronic transaction. The buyer is now an active player that can decide whether to trust or not in the entity that issues the signature policy and to accept or not the terms established in it. On the other side, the seller can publish the conditions under which any potential buyer must adhere to in order to buy a resource in its e-commerce scenario. As a result, the main contributions of our protocol are the increase of the user's confidence in e-commerce and to allow the seller to customize the way others must participate in its business processes.

Previous protocols in the literature focused only on assuring the fairness and timeliness of the protocol, at the same time that they tried to improve the overall performance by decreasing the number of cryptographic operations. However, these protocols do not place themselves in real e-commerce environments, where the user obviously plays an important role. In our approach, by enhancing the trust in the transaction security and fairness, the most difficult obstacle in e-commerce can be overcome: the user's confidence.

On the other hand, our protocol has been designed to be compliant to European and International electronic signature standards, what assures that a solution based on this protocol will be interoperable with other standard e-commerce frameworks, and can be quickly implemented and put on practice.

The rest of the paper is organised as follows. In next section key concepts and basic notation used for describing the protocol are defined. Section 3 reviews the signature policy concept. The optimistic fair exchange protocol is detailed in Section 4. Section 5 analyses the overall security of the protocol, in an attack-countermeasure approach. Dispute resolution is detailed in Section 6. Section 7 discusses

implementation guidelines. Finally, Section 8 contains the article conclusions.

2. Basic concepts and notation

2.1. *Basic concepts*

Next, the basic concepts for the article are explained:

- Digital signature

''Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source of the data unit and protect against forgery, i.e. by the recipient'' (ISO 7498-2, 1989).

- Electronic signature

''Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication'' (Directive 1999/93/EC, 1999).

If non-repudiation is needed to be achieved, it is of paramount importance to incorporate additional information to the electronic signature and fulfil certain requirements during its generation. Under the scope of Directive 1999/93/EC (1999), these signatures are called advanced electronic signatures.

- Non-repudiation of origin (NRO)

Electronic signature of a message carried out by the origin of the communication, and which provides the receiver with proof of origin of the message, protecting against any attempt by the originator to falsely deny having sent the message (Zhou and Gollmann, 1996a).

In e-commerce context the origin is normally the buyer. In the proposed protocol, and from now on, the buyer will be referred as the origin, and the NRO will be generated over the resource order and the origin's credit card information.

- Non-repudiation of receipt (NRR)

Electronic signature of a message carried out by the receiver of the communication, and which provides the origin with proof of receipt of the message, protecting against any attempt by the recipient to falsely deny having received the message (Zhou and Gollmann, 1996a).

In e-commerce context the receiver is normally the seller. In the proposed protocol, and from now on, the seller will be referred as the receiver, and the NRR will be generated over the resource order and the origin's credit card information, acting as an acknowledgement of receipt.

- Non-repudiation of acknowledegment (NRA)

Electronic signature of a message carried out by the receiver of the communication, and which provides the origin with proof of acknowledgement, protecting against any attempt by the recipient to falsely having acknowledged the message.

In this case, both the buyer and seller could be the receiver of the message. In the protocol proposed in Section 4, the NRA will be generated by the origin over the NRR.

- Trusted Third Party (TTP)

A system, platform or individual trusted by the players of a transaction (origin and receiver) and which acts in a fair manner during the protocol execution.

- Fair exchange protocol

An exchange protocol which ensures that no participant gains an unfair advantage over the other during the protocol execution.

- Timeliness fair exchange protocol

During any stage of the protocol, both players can achieve, in a finite amount of time, a point to leave the protocol without needing the participation of the other player, and where both participants are placed in a fair situation over each other.

- Optimistic fair exchange protocol

A fair exchange protocol which assumes that both players will not misbehave, and during which the TTP is only required when this assumption is broken by any of the players. In this case, the TTP is known as an offline TTP.

2.2. *Notation*

The following basic notation is used throughout the paper:

- S.P.

Signature policy S.P.

- $X \rightarrow Y : m$

Entity X sends message m to entity Y.

- $X \leftarrow Z$: S.P.

Entity X retrieves signature policy S.P. published by entity Z.

- Sx (m, S.P.)

Electronic signature generated by entity X over message m and based on signature policy S.P.

- NRO = Sx (m, S.P.)

Non-repudiation evidence of origin (entity X). It is an electronic signature generated over m under S.P. conditions.

- NRR = Sy ((m, NRO), S.P.)

Non-repudiation evidence of receipt (entity Y). It is a sequential parallel signature (see Section 3.2 for definitions),

carried out by Y over m (after NRO) and generated under the conditions established in signature policy S.P.

- NRA = Sx (NRR, S.P.)

Non-repudiation evidence of acknowledgement (entity X). It is an embedded electronic signature (see Section 3.2 for definitions) generated by X over NRR under S.P. conditions.

3. Signature policies

3.1. *Concept*

The signature policy concept was introduced by ETSI, the European Telecommunications Standards Institute, and later adopted by IETF, the Internet Engineering Task Force. According to (ETSI TR 102 041, 2002), a signature policy (S.P.) is a document that collects a set of rules to create and validate electronic signatures, under which an electronic signature can be determined to be valid in a particular transaction context. The document can be written in an informal text form provided the rules of the policy are clearly identified or using a formal notation like ASN.1 (ETSI TR 102 271, 2003) or XML (ETSI TR 102 038, 2002). In the former case, there will be a requirement of human interaction at the time of differentiating if the signature is valid or not, while in the latter it is possible to automatically validate it, by using suitable programs.

There are several bodies that ease the work with signature policies. These bodies can be divided into:

- Signature Policy Issuers

Entities that define the technical and procedural requirements for electronic signature creation and validation, in order to meet a particular business need.

- Signature Policy Publication Authorities

Entities in charge of publishing and making the signature policies description available to users while the signature policies are still valid.

- Signature Policy Archiving Authorities

Signature Policy Issuers may disappear once they have issued their policies and Policy Publication Authorities are not obliged to maintain the signature policies after they expire. But users may still want to validate electronic signatures created under a signature policy a long time after its expiration date. The task of archiving the signature policies in a publicly accessible repository is done by Signature Policy Archiving Authorities.

Basically, an S.P. contains the following information:

- The S.P. unique Object Identifier (OID).
- Information about the Signature Policy Issuer.
- Field of application of the S.P. It refers to legal, contractual or application contexts in which the signature policy is to be used and the specific purposes for which the electronic signature is to be applied.
- The Signature Policy Validation section, which defines, for the signer, the data elements that shall be present in the electronic signature that is generated and, for the verifier, the data elements that shall be present for an electronic signature to be potentially valid under that signature policy. Validation information can be time stamps (IETF RFC 3161, 2001), Online Certificate Status Protocol (OCSP) responses (IETF RFC 2560, 1999), Certificate Revocation Lists (CRLs) (IETF RFC 3280, 2002), etc.
- Constraints for generating electronic signatures: use of smartcard, use and management of attribute certificates, etc.
- Constraints for electronic signatures validity generated under this S.P.: maximum validity period for the generated signature, grace period, etc.
- Commitment type made by the signer in relation to the signed data: proof of origin, proof of receipt, legal commitment, notary, witness, proof of acknowledgement, etc.

As it can be seen in the commitment type field, signature policies include origin and receiver roles, and thereby its use in a fair exchange protocol is rather suitable.

It is worth noting that the S.P. (or a reference to it) is a signed attribute inside an electronic signature (ETSI TS 101 733, 2007; IETF Draft, 2007; ETSI TS 101 903, 2006; W3C XML), and therefore is not possible to substitute the policy used during the signature generation without invalidating such signature. This prevents the possible situation where an attacker wants to limit the requirements under which the signature is considered to be valid by replacing the policy by a less demanding one.

3.2. *Using signature policies in complex business models*

Previous information is normally focused on the generation/validation of a single electronic signature. However, there are complex business models where several electronic signatures must be applied because a single one is not enough for covering the business needs. Multiple electronic signatures appear to fulfil those requirements. Next, two important use cases that need multiple signatures are listed:

- A document must be electronically signed by two or more people/entities.
- An electronic signature must be signed (authorized) by another person/entity or people/entities.

The first use case needs what are called co-signatures, also known as parallel signatures. They are mutually independent signatures where the ordering of the signatures is not important. They are directly applied to the document. There is a variation where the order of the parallel signatures is significant. These signatures are called sequential parallel signatures. The second use case requires counter-signatures or embedded signatures. In this case one signature is applied

to another. The sequence in which the signatures are applied is important and there is a strong interrelationship.

By combining these three types of signatures, all needs related to electronic signatures can be covered.

In ETSI TR 102 045 (2003) the S.P. model described in ETSI TR 102 041 (2002) is extended for dealing with complex business models that need multiple signatures.

4. Optimistic fair exchange protocol based on signature policies

The objective of the protocol is the fair exchange of origin's message and non-repudiation evidence of both origin and receiver in an e-commerce context. The protocol is divided in two protocols, the main and the recovery protocols, and makes use of two timeouts, timeout t_0 and timeout t_1. The rules that manage the protocol execution, as well as the timeouts values and dispute resolution clauses are specified in the signature policy. Therefore, the exchange between origin and receiver (and TTP when necessary) totally depends on the signature policy content.

The main protocol, explained in Section 4.2, allows the exchange of origin's message and the non-repudiation information, including the final evidence, the NRA (see Section 2.2). Neither NRO nor NRR is considered as valid evidence on their own for claiming the other payer's commitment in the transaction. The signature policy determines that only the evidence NRA can be considered as the valid one, tying down both origin and receiver in the transaction. Therefore, the signature policy S.P. will set a rule that, if no NRA has been properly generated, then no responsibility can be claimed in a future dispute.

The recovery protocol, detailed in Section 4.3, allows achieving the fairness and timeliness of the protocol in case of errors during the execution of the main protocol or due to players' misbehaviours. Therefore, this protocol is only executed under certain circumstances, and it is the only stage where the TTP participates.

During the protocol execution time references are included in the signatures. These time references, in conjunction with the timeouts defined in the S.P., allow detecting if players are behaving properly or if it is necessary to execute the recovery protocol. Such time references consist in time stamps generated by a TTP playing the role of a Time-Stamping Authority (TSA) (IETF RFC 3161, 2001). A time stamp is calculated over the digital signature value. For simplifying the protocol description, the process of time stamping the signatures is not included. A brief description of the protocol timeouts is given in Section 4.4.

Finally, Section 4.5 contains a brief technical description of a signature policy oriented for this protocol.

4.1. *Entities of the protocol*

Before formally detailing the protocol, the function of each participant entity is briefly explained:

- Origin (O)

It is the entity that sends the message to the receiver with the corresponding electronic signature, which acts as the proof of origin (NRO). It waits for the proof of receipt of the message.

The origin also needs to perform the proof of acknowledgement (NRA), which is an embedded signature generated over the NRR.

- Receiver (R)

It is the entity that receives the message and the corresponding NRO. Once the NRO has been validated, the receiver applies a sequential parallel electronic signature to the message. This signature is then sent to the origin as the proof of receipt (NRR).

- TTP-SP

It is a Trusted Third Party which, in our protocol, acts as both the Signature Policy Issuer and the Signature Policy Publication Authority, according to ETSI TR 102 041 (2002). Normally, these roles are held by different entities, but other configurations are possible if desired. In the protocol the TTP holds both roles in order to make the explanation clearer. The TTP-SP has certain signature policies configured and available both to the origin and receiver.

- TTP

It is a Trusted Third Party which participates in the recovery protocol. Thus, it acts in optimistic mode, that is, only when an abnormal situation occurs in the main protocol.

4.2. *Main protocol*

This protocol has the following steps (see Section 2.2 for notation):

1. O ← TTP-SP : S.P.
2. O → R : NRO, m
3. R ← TTP-SP : S.P.
4. R → O : NRR
5. O → R : NRA

In the first step the origin accesses the TTP-SP to obtain the proper S.P. Subsequently, in step 2, the origin generates and sends to the receiver the electronic signature applied to the message m (the resource order and his/her credit card information). This signature acts as the NRO. The electronic signature is performed under the terms of the S.P.

Once the receiver has received m and NRO in step 3, it accesses the TTP-SP to obtain the referenced S.P. By using the same S.P., the receiver validates the NRO. In step 4 the receiver generates and sends the NRR, which consists in a sequential parallel signature applied to m. The NRR represents the acknowledgement of receipt for message m. The sequence in which these parallel signatures have been applied is important, and should be defined in the S.P. – the NRR must be applied after the NRO.

In the last step the origin must validate the NRR received, according to the S.P. After that, the origin generates the last signature of the protocol, called NRA, which is an embedded

signature applied over the NRR. By this action, the origin acknowledges the completion of the protocol.

4.3. *Recovery protocol*

Notice that the origin can generate the NRA (step 5) without sending it to the receiver.

For allowing the receiver to obtain the complete evidence, next recovery protocol is proposed:

1. R → TTP : NRR, NRO
2. TTP ← TTP-SP : S.P.
3. TTP → R : NRA
4. TTP → O : NRA

In step 1 the receiver sends the NRO and NRR to the TTP.

Then, the TTP must access to the TTP-SP (step 2) in order to retrieve the referenced S.P. After the validation of both signatures, the TTP generates an NRA over NRR.

In the last two steps the TTP delivers the NRA to both the origin and receiver. The public certificate associated to the private key used by the TTP must be set in the S.P. as a valid certificate for generating NRAs.

4.4. *Protocol timeouts*

Two timeouts, t_0 and t_1, play an important role in the protocol, and therefore must be defined in the S.P.

Timeout t_0 establishes the time the receiver must wait before executing the recovery protocol. Thus, the receiver is the only one that can execute the recovery protocol.

Timeout t_1 avoids the receiver and the origin to perform specific attacks on the protocol. These attacks are further detailed in Section 5.

A requirement to be fulfilled by these timeouts is that t_1 must be higher enough than t_0 for allowing the receiver to complete the recovery protocol.

4.5. *Technical overview of a protocol-oriented signature policy*

As previously said, the signature policy S.P. is the key element of the protocol, as it contains all information needed by the parties (origin, receiver and TTP) to follow the steps of the protocol and to know what to do in each on them. This section gives a brief technical overview about the composition of the signature policy S.P., covering the main information that manages the protocol execution.

First of all, the signature policy should contain a description about the receiver's business context where electronic signatures generated under the policy are considered as valid.

The core of the signature policy S.P. is composed of possible signers' roles and type of electronic signature (sequential, sequential parallel, and embedded) to be generated by each one. Additional data to be appended to each signature can also be described, like timestamps or validation information. The most important aspect of the core relates to the audience conditions, that is, what is considered as valid evidence of the performed transaction (the NRA). This information must explicitly state what electronic signatures generated by which roles compose the final evidence.

Another important aspect is related to the supported authorities: certification authorities, time-stamping authorities, CRL issuers, etc. This gives a more specific view to the user about the parties that will have some part of implication in the protocol execution. Therefore, the overall trust can be balanced better by the user.

Timing constraints (timeouts t_0 and t_1) must also be specified.

Finally, the signature policy must cover dispute resolution clauses and procedures.

An example of a signature policy for the protocol written in informal language can be seen in the Appendix.

5. Protocol analysis

This section analyses the security as well as fairness and timeliness characteristics by evaluating several attacks on the protocol and their countermeasures. The attack method can vary, but the attacker's objective mainly remains the same: to obtain valid evidence from the other side without making any commitment in the transaction.

Four types of attack are evaluated. First three attacks are considered as the main methods an attacker could use for achieving valid evidence due to the protocol design. Last attack analysis phishing as a representative example that highlights the vulnerability of a web site that does not provide a proper web server identification and authentication. Although this type of attack is not directly related to the protocol design, and rather to how the protocol is implemented and deployed, two possible solutions are provided to cover this security issue.

Timeouts t_0 and t_1 will strongly depend on communication conditions, as well as on electronic signatures generation and validation processing times. Therefore, temporal slot assigned for each action in following figures is for illustrative purpose only.

5.1. *Attacks based on protocol interruptions*

This kind of attacks consists of aborting the protocol in a chosen step. Notice that sometimes a communication or system error can cause the same effect.

There are mainly three possible attacks in this category:

- Main protocol interruption after NRO reception

The receiver stops the protocol at step 2, causing the origin not obtaining any evidence from the receiver.

However, due to the conditions established in S.P. rules, which dictate that only the NRA is the valid evidence, the receiver could not make use of NRO as a valid one.

- Main protocol interruption after NRR reception

The origin stops the protocol at step 4 and after receiving the NRR. Therefore, the receiver possesses the NRO and the origin the NRR.

For the same reason as before, this evidence cannot be considered as complete.

- Main protocol interruption after NRA generation

The origin stops the protocol at step 5 after generating the NRA. This situation places the receiver at an unfair position. The origin possesses the valid evidence while the receiver only has the NRO and NRR.

For counteracting this origin's misbehaviour, the receiver must execute the recovery protocol once timeout t_0 has passed, as explained in Section 4.3.

5.2. *Receiver's delay attack*

In this attack, the receiver tries to be the only one that obtains the valid evidence NRA by forcing the origin to abandon the protocol.

The method consists of provoking a long delay after NRR generation. If the origin supposed, for example, that there has been a communication error during NRO sending, he would abandon the protocol. Afterwards, the receiver could successfully execute the recovery protocol, obtaining the NRA while the origin does not. Fig. 1 represents this *receiver's delay attack*.

For avoiding this unfair situation for the origin, the TTP must consider the elapsed time since the origin generated the NRO until the NRO and NRR are received from the receiver at step 1 of recovery protocol. If this elapsed time is higher than the established timeout t_1, the TTP must send an abort message to both the origin and receiver. Notice that the time reference used by the TTP is the moment when it receives the NRR and NRO, not the NRR generation moment. If not, and because the receiver generates the NRR before provoking the delay, the elapsed time would be smaller than t_1, and then the TTP would accept the recovery protocol execution. Fig. 2 shows how the TTP must prevent the receiver's delay attack by checking the elapsed time from NRO generation to NRR/NRO reception (not NRR generation).

An important condition can be deduced from previous figure. If the origin decides to abandon the protocol, he must wait at least a time equal to t_1. If not, the receiver could successfully execute the recovery protocol after just a small delay.

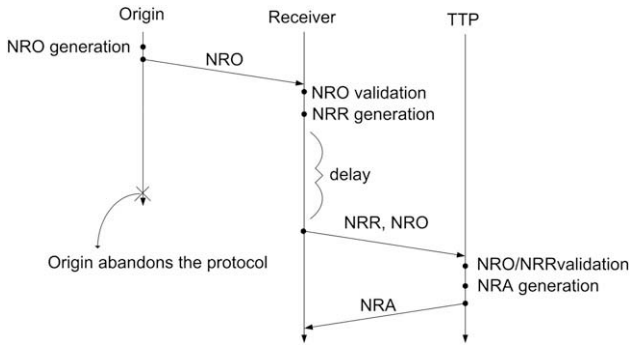

Fig. 1 – Receiver's delay attack.

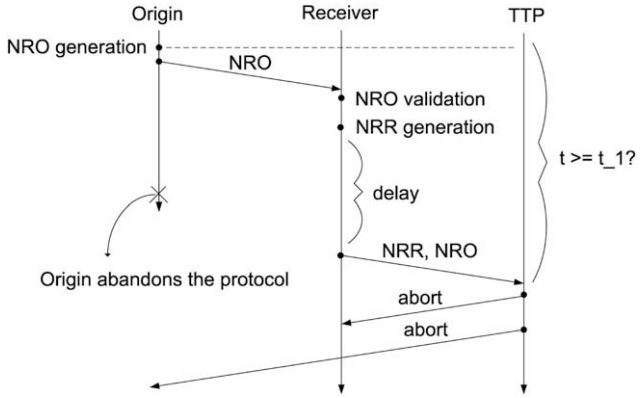

Fig. 2 – TTP's verification for preventing receiver's delay attack.

5.3. *Origin's delay attack*

There is another possible attack that we have called *origin's delay attack*. In this case, the attacker is the origin, and, like in the receiver's delay attack, the aim is to be the only one who obtains the valid evidence NRA.

However, the method used in this attack is different. Instead of forcing the receiver to abandon the protocol, the origin will try to cause an enough delay in order to forbid the receiver from executing the recovery protocol.

More specifically, the origin generates the NRO and waits at least t_1 before sending it to the receiver. Once the origin has generated the NRA at step 5 of main protocol, it aborts the protocol. When the receiver tries to execute the recovery protocol, the TTP will reject it due to t_1 timeout. This attack is represented in Fig. 3.

For countering this attack, the receiver must check that the elapsed time since the NRO generation until it is received and validated is less enough than t_1. If this condition is not fulfilled, the receiver must stop the protocol.

5.4. *Phishing*

This section covers phishing as an example of an attack which makes use of how the protocol has been implemented and deployed.

In phishing, the attacker masquerades as the original vendor's web site for obtaining sensitive information from its customers, such as their credit card information or their access credentials. Particularly, in this protocol an attacker could try to obtain origin's sensitive information by masquerading as the trustworthy receiver in the electronic transaction. For that, the attacker would create a fake online web site similar to the receiver's one, and then would invite the origin to initiate the online purchase on its web site – for instance, by sending an e-mail. Afterwards, the origin would send to the attacker his/her sensitive information (e.g. credit card information) along with the NRO. The attacker could then make use of this information for malicious purposes without the origin's consent.

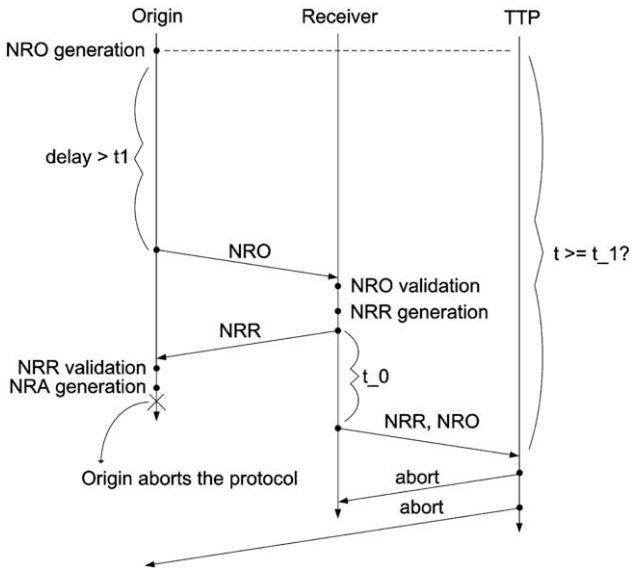

Fig. 3 – Origin's delay attack.

This attack is possible since the protocol does not authenticate each entity before starting the messages exchange. The reason is that the main purpose of the protocol is the fair exchange between origin and receiver, and then prior entity authentication is not covered in its design.

However, this security issue could be solved by implementing one of these two possible mechanisms:

- Setting the transaction on a SSL/TLS channel. By this way, the origin could verify the receiver's certificate before starting the protocol, and also check that this certificate is the same as the one specified in the signature policy (also available before starting the protocol).
- Encrypting the information exchanged in each step with the public key of the other entity. That is, the origin would encrypt his/her sensitive information with the public key contained in the receiver's certificate specified in the signature policy. If the recovery protocol had to be executed, the receiver would encrypt the information with the TTP's public key, also extracted from the certificate specified in the signature policy. As an extra security procedure, the TTP would encrypt the NRA with the corresponding public key before sending it to the origin and the receiver. By these measures, only the authorized entity could have access to the information in each step of the protocol.

Besides resolving the phishing attack, both solutions also enhance the protocol by providing confidentiality to the exchanged information. However, although the SSL/TLS-based solution is completely transparent to the protocol design, it does not provide origin's sensitive information confidentiality between the receiver and the TTP. For this, another SSL/TLS channel should have to be established between these two entities. Second option implies modifying the protocol design, but, on the other hand, provides confidentiality throughout the whole protocol execution. Another advantage of this solution is that sensitive information can always be kept encrypted, even in the receiver's purchase orders database.

6. Dispute resolution

An important issue in fair exchange protocols is the dispute resolution, which has to be carried out in two cases:

- If the receiver claims to have received message m while the origin denies having sent it to the receiver.
- If the origin claims to have sent message m while the receiver denies having received it from the origin.

The dispute resolution objective is to settle who is lying and who is saying the truth. For that purpose, evidence collected during the protocol execution must be evaluated by a fair and neutral third party, for instance, a judge. This judge is normally a physical person who, by using the appropriate software, can determine the validity of the evidence.

In this protocol, and in both previous cases, the evidence that must be presented to the judge is the NRA, which must have been generated according to protocol requirements and the signature policy rules. The protocol design assures that either both parties obtain the NRA or none of them can gain any advantage over the other. The NRA can have been generated either by the origin or the TTP.

Therefore, the judge must verify the correctness of the NRA, in the sense of digital certificates used by the parties, the validity of the digital signatures and the rest of the information that should have been included in the evidence (see Section 7 for further information), always according to the signature policy statements.

The existence and correctness of this evidence determines whether the claims of origin or receiver are right or wrong.

7. Implementation guidelines

This section contains implementation guidelines and recommendations about signature formats to use, methods for obtaining the validation information and a signature policy architecture proposal that can be integrated in the protocol design. Also, assumptions on communication channels are provided.

7.1. *Signature policy architecture*

In Section 3.1, different entities have been defined: the Signature Policy Issuer, the Signature Policy Publication Authority and the Signature Policy Archiving Authority. Each entity carries out a specific task in signature policy architectures. In this section the general architecture in which the proposed protocol should take place is explained in more detail.

One of the key entities in the architecture is the Signature Policy Publication Authority. This entity allows both buyer and seller access a repository for retrieving the signature policy to be used during the protocol execution. The Signature Policy

Archiving Authority may also be present in order to allow signature validations even a long time after the signature policy expiration date. The role of the Signature Policy Issuer is not needed during the protocol execution, but obviously it is necessary before the protocol can take place. The issuer can be a legal person (i.e. an organization) or a natural person (acting under a professional function) that establishes the rules that must be followed by his/her community of users when generating/validating electronic signatures. Publication task can be carried out by the Issuer as well.

Next figure shows an architecture where above roles are played by three different independent entities. The issuer entity is an external organization to which the receiver is adhered.

As it can be seen in Fig. 4, the receiver communicates with the Issuer for selecting, among all available policies, the signature policy to be used during the protocol execution. Issuers are normally linked to receivers, and sometimes the receiver generates its own policy. In a normal scenario it is the receiver the one who imposes the requirements for buying a resource in his/her (e-)commerce. Obviously, the origin can decide whether to accept or not these requirements, by reviewing the signature policy rules and specific receiver's web site conditions.

After that, the seller has to make the signature policy available to origins. For that purpose the signature policy is uploaded to the Publication Authority repository. Once buyers and seller can obtain the signature policy, the fair exchange protocol can be launched.

It is important to remark that while the signature policy is still valid, the players can retrieve the signature policy from the repository located at the Publication Authority in order to create and validate the signatures. Once the signature policy has expired, the Publication Authority should forward it to the Archiving Authority, allowing the signatures to be validated beyond the end of the validity of the signature policy (e.g. a judge has to perform a dispute resolution). However, no more signatures should be created under the rules of an expired signature policy.

7.2. *Assumptions on communication channels*

The architecture proposed in Fig. 4 implies several message transmissions among involved parties. This section sets out the communication channel assumptions made by the authors.

Communication channels are usually categorized as follows (Shao et al., 2006):

- Unreliable channel. A channel that may not deliver messages randomly.
- Resilient channel. A channel that reliably delivers any message to the other end, after some finite but unknown amount of time.
- Reliable channel. A channel that delivers any message to the other end after a fixed and known delay.

Next, all communication channels in the protocol are analysed using previous classification and the minimum requirements of each communication channel are discussed:

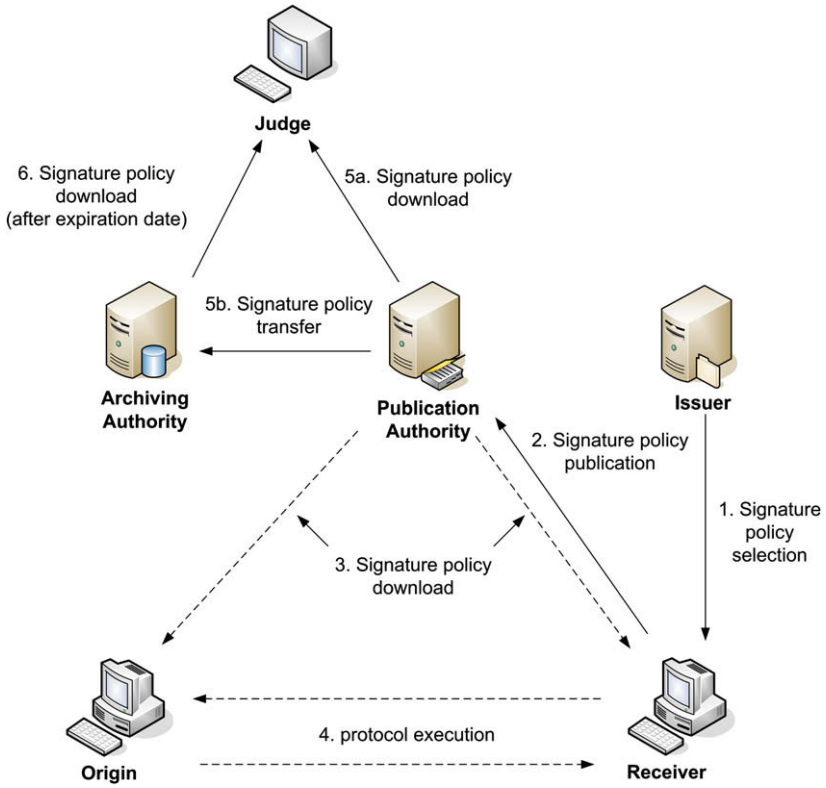

Fig. 4 – Signature policy architecture.

(a) Receiver ← Issuer

This channel is used by the receiver for downloading the signature policy file. Because the receiver will make as many attempts as necessary for successfully downloading the file, even an unreliable communication channel could be used.

(b) Origin ← Publication Authority

This channel is needed only once for performing the NRO according to the signature policy. From that point onward, the origin uses the downloaded policy for NRR validation and NRA generation. Because it is assumed that the origin will try to download the signature policy until successfully obtained, a reliable, resilient or unreliable communication channel could be used.

(c) Receiver ← Publication Authority

Once the protocol is started, delays at message receptions are taken into account. For avoiding the origin abandonment, it is recommended to use a reliable communication between the receiver and the Publication Authority. If this requirement cannot be fulfilled, then a resilient channel could be used provided that timeouts t_0 and t_1 are configured accordingly.

(d) Origin ↔ Receiver

During the protocol execution, communication errors that could cause messages losses are taken into account by using timeouts t_0 and t_1. Same justification as previous point (c) applies here.

(e) Archiving Authority ← Publication Authority

Signature policy transference from the Publication Authority to the Archiving Authority requires a communication channel with a high level of reliability, that is, either a reliable or resilient communication channel.

If an unreliable communication were used, the signature policy could not be successfully sent to Archiving Authority (e.g. if an error in the transference occurred and the Publication Authority deleted the file from its repository), and thus no electronic signature generated under this signature policy could be validated anymore.

(f) Judge ← Publication Authority and Archiving Authority

Finally, this case can be argued to be exactly the same as (a), so it is supposed that the judge will make as many attempts as necessary to successfully download the signature policy.

Table 1 summarizes minimum requirements for existing communication channels.

Table 1 – Minimum requirements for communication channels in the protocol architecture

Communication channel	Minimum requirement
Receiver ← Issuer	*Unreliable*
Origin ← Publication authority	*Unreliable*
Receiver ← Publication authority	*Resilient* *Reliable (recommended)*
Origin ↔ Receiver	*Resilient* *Reliable (recommended)*
Archiving authority ← Publication authority	*Resilient*
Judge ← Publication authority/ archiving authority	*Unreliable*

7.3. *Electronic signature format*

Evidence exchanged during the protocol consists of electronic signatures. An electronic signature assures message integrity and authenticity. As explained in Section 2.1, if the context requires the assurance of non-repudiation of the actions performed, as it is the case in the proposed protocol, it is of paramount importance to incorporate additional information to the electronic signature and fulfil certain requirements during its generation.

Assuring specific conditions (i.e. the data to be signed is not modified during signature generation, the document to be signed is shown to the signer before the signature is computed, the private key has not been compromised, etc.) during signature creation is maybe one of the most difficult tasks to achieve in PKI and e-signature applications, and is not under the scope of this article. However, the information that must be added to the signature in order to strengthen its validity is, indeed, the goal of this section.

The main aim is to provide electronic signatures with all necessary information that allows them to be successfully verified in the future, even if a long time has passed since their creation. The reason is that in e-commerce context, electronic transactions usually relate to contractual operations. More specifically, in this article a context where a buyer and a seller make a commitment about a purchase order has been presented. It is possible that this commitment should still be valid long time after the transaction took place (i.e. dispute resolution).

Advanced electronic signature (AdES) formats are the solution for this necessity. AdES formats are grouped in CAdES (ETSI TS 101 733, 2007; IETF Draft, 2007) or XAdES (ETSI TS 101 903, 2006; W3C XML), if defined in ASN.1 (ISO/IEC 8824-1, 2002) or XML (W3C Recommendation, 2006), respectively. These formats have been proposed by three major standardization organisations (ETSI, IETF and W3C World Wide Web Consortium) and are widely accepted for providing e-signatures with long term validity. Different AdES formats have been defined according to the required degree of reliability: AdES-T (with Time-stamp), AdES-C (with Complete validation data), AdES-X (with eXtended validation data) and AdES-A (with Archive validation data), quoted from lower to higher degree of reliability.

Signature policies (ETSI TR 102 041, 2002) have been defined both in ASN.1 (ETSI TR 102 271, 2003) and XML (ETSI TR 102 038, 2002). This allows its use in CAdES and XAdES. Incorporating a signature policy (or a reference to it) in an AdES upgrades it to an AdES-EPES format (Explicit Policy-based Electronic Signature), a format from which AdES-T, AdES-C, AdES-X or AdES-A can also be built.

Specifically, we suggest an AdES-EPES format (either in XML or ASN.1) that contains following validation information:

- Timestamp over the digital signature value.
- Certification path.
- Certificates revocation status information.

Time stamping a digital signature provides evidence that the signature has been created before the time of stamping, and requires the presence of a Time-stamping Authority (TSA). Certification path implies capturing all the certificates from the certification path, starting with those from the signer and ending up with those of the self-signed certificate from one trusted root. By this, the verifier can ascertain that the certification path was valid according to naming or certificate policies constraints. Finally, revocation status information of all certificates presented in the signature completes it with the necessary information for assuring its validity in a future, although this information could not be obtained anymore. Revocation information can be obtained by accessing the OCSP service of the corresponding Certification Authority (CA), if available, or by retrieving the CRL if not.

Validation information above provides the electronic signature with long term proof. By combining time reference with certification path and revocation status information, verifiers can be sure, at any time (even after certificate expiration or revocation), about the validity of the signature and signer's certificate at the moment of signature generation. Note that a CA normally deletes a certificate revocation information entry from the CRL as soon as the certificate expires.

Moreover, the AdES-EPES allows the generation of electronic signatures according to a signature policy, complying with the conditions imposed by the optimistic fair exchange protocol proposed in this article.

7.4. *Addition of validation information*

Previous information may be collected and added to the signature by the signer or verifiers, depending on the context and particular technological limitations.

For instance, if the signer is an individual buyer with limited computer capability, then it is preferable to move the validation information retrieval from the buyer to the seller side.

In case the transaction is performed in a B2B context, assuming that both sides are able to access external systems and none of them have network bottlenecks, the solution is not fixed either. The protocol proposed in this article sets that each side must obtain a time reference for the signatures they generate. By this way, because the timestamp is obtained before sending the electronic signature, a more accurate time reference is applied by avoiding communication delays. However, it is also possible to establish that each one must obtain the validation information of the other side, in order to be sure that, for example, the revocation status information corresponds to the validation time reference and therefore has not been obtained before the signature generation. Notice that a grace period should be taken into account for allowing revocation requests being processed by the Certification Authorities before the verifier collects the revocation information. If not, the verifier will not obtain reliable information if a revocation request was issued by the signer just before the signature was computed and time stamped (ETSI TS 101 733, 2007; ETSI TS 101 903, 2006). Obviously, there must be coherence between the grace period and t_0 and t_1.

The solution that fits better with the protocol design is a hybrid one. On one hand, each side obtains a timestamp over the digital signature it has just generated and adds it to the AdES-EPES, building an AdES-T. On the other hand, the other side must collect the remaining validation information after the AdES-T has been validated. As an example, in step 3 of main protocol the receiver must verify the NRO with timestamp, and then, if successfully verified, collect the certification chain and the revocation status information of all included certificates. On the other hand, in step 5 the origin must do the same with the time stamped NRR and receiver's related certificates.

This solution improves the accuracy of the validation information while preserving the closest time reference of each signature. If the communication between buyer and seller has to be as interactive as possible, then no grace period should be applied. Trade-off between accuracy and time-response must be made by the system designer.

The way the validation information (certification path and revocation status information) is added to the AdES-T differs, and depends on specific implementation conditions. There are mainly two possibilities: incorporating the validation information itself (AdES-X) or incorporating a reference to it (AdES-C). The former solution allows the AdES being completely independent but of greater size, while the latter minimizes the size of the resulting signature but obliges to store the information in an accessible repository. Due to the need of specific applications for storing referenced information in an AdES-C solution, in a B2C context an AdES-X solution is probably a better choice. In B2B both solutions could be applied.

8. Conclusions and future work

E-commerce is prone to generate situations where buyers are at a disadvantage to sellers. Particularly, this article has analysed the situation where a buyer, after sending his/her sensitive information together with the proof of origin to the seller, expects to receive the corresponding proof of receipt. There is a moment when the seller has all necessary evidence from the buyer but without having made any type of commitment. For resolving this unfair situation, different protocols have been proposed so far, during which neither buyer nor seller can gain any advantage during the electronic transaction. These protocols are known as fair exchange protocols.

In this article a completely new and innovative fair exchange protocol has been proposed. The protocol is based on signature policies, a concept recently introduced by the European Telecommunications Standards Institute (ETSI), and which collects the set of rules under which an electronic signature can be determined to be valid in a particular transactions context. The security, fairness and timeliness

characteristics of the protocol have been evaluated, proving that main feasible attacks to its design are counteracted. It is also worth mentioning that the protocol design with an offline TTP improves the overall performance provided that no misbehaviour occurs.

By using this approach, the buyer can decide if trusting or not in the entity that issues the signature policy and if accepts or not the terms established in it. This new contribution in fair exchange protocols allows increasing the confidence in e-commerce, because the buyer is now an active player that knows and evaluates the conditions that will manage the electronic transaction. Once the trust relationship has been set, the protocol ensures that either both parties obtain the valid evidence or none of them gains any advantage over the other. In case that a dispute arises about what actually happened during the transaction, evidence must be provided to a judge.

On the other hand, compliance to European and International electronic signature standards assures that a solution based on this protocol will be interoperable with other standard e-commerce frameworks, and can be quickly implemented. For easing implementation processes, general guidelines covering key factors have also been widely explained. As it can be noticed in Section 5.4, protocol implementation and deployment is quite important since some relevant attacks can be counteracted by applying complementary security measures, such as using SSL/TLS channels between each entity. IT staff that wants to put this protocol proposal in practice must take these factors into account if they want to provide a secure implementation of the protocol.

Future work will be focused on three main objectives. First of all, a prototype of the protocol will be developed, permitting discovering any possible vulnerability not detected yet. Performance testing will also help to enhance the protocol by highlighting any bottleneck in the design. Finally, current TTP will be replaced by a transparent TTP (Markowitch and Kremer, 2001; Wang, 2006). If a transparent TTP is used, nobody can discover if the TTP intervened of not, thus avoiding bad publicity to the parties in cases when a network failure occurs instead of a party misbehaviour.

Appendix. Signature policy example

This appendix contains a signature policy example written in an informal manner that could be used in an e-commerce transaction which uses the Optimistic Fair Exchange Protocol proposed in the article.

This signature policy is a fictitious example of a book shop that sells books through the Internet. The important aspect to remark is that this signature policy considers all conditions needed by the protocol. Only the electronic signatures generated under this policy terms and therefore that fit the protocol requirements are considered to be valid.

Title/identification of signature policy:

Alice Bookshop Signature Policy for use in the provision of the Internet book shop service to consumers.

Version No: 1.0.

Date: 17/07/2007.

Business application domain:

This policy covers the provision of the Internet book shop service provided by Alice Bookshop to its consumers.

Transactional context:

Purchase Order/Acceptance in relation to a book purchase order made through Alice Bookshop Internet Web page between Alice Bookshop and a client of Alice Bookshop.

Consent to accept electronic signatures:

Alice Bookshop agrees that it will accept signatures in electronic form which comply with this policy.

Proposed signers:

On behalf of Alice Bookshop client

The book orders shall be signed as proof of origin by any person acting as an Alice Bookshop client.

The proof of acknowledgement shall be an embedded signature performed over the proof of receipt by the person acting on behalf of the Alice Bookshop client.

Both the proof of origin and the proof of acknowledgement shall be generated by using the same certificate.

On behalf of Alice Bookshop

The book orders shall be signed as proof of receipts by Alice Bookshop signature creation system on behalf of Alice Bookshop, with the Certificate with Serial Number 12345 and issued by Certification Authority YYYY.

The proof of receipt shall be a parallel signature performed over the book order and after the proof of origin.

Signature commitment types:

1. Proof of origin;
2. Proof of receipt;
3. Proof of acknowledgement.

Timing constraints:

The recovery protocol shall be initiated 2 min after the proof of receipt has been generated and sent to the client.

The TTP shall reject any recovery protocol initiated 4 min after the proof of origin was created.

Specifications (at high level) of any security considerations:

All signatures shall conform to article 5.1. Electronic Signatures Directive 1999/93/EC; and all certificates shall be qualified certificates and issued by a qualified certification authority.

It also shall be deemed sufficient proof of acknowledgement signatures created by the Trusted Third Party (TTP) ZZZZ, with the Certificate with Serial Number 54321 and issued by Certification Authority XYZ.

All signatures shall be time stamped by any TSA which conforms to Certificate Service Provider conditions established in Directive 1999/93/EC for Electronic Signatures.

All signatures must include, at least, the following validation data:

- Complete certificate and revocation references (OCSP Responses and/or corresponding CRLs).

Allocation of responsibility for signature verification/validation:

Alice Bookshop client's signature and TTP's signatures shall be validated by Alice Bookshop signature validation system, or any relying party selected by Alice Bookshop.

It is Alice Bookshop client responsibility the validation of Alice Bookshop's and TTP's signatures.

TTP shall validate any received signature; either it belongs to any Alice Bookshop client or to Alice Bookshop itself.

Audience conditions:

The purchase order and the corresponding receipt shall not be valid or binding upon Alice Bookshop nor its clients unless the following conditions are fulfilled:

- The purchase order shall be signed by the client acting as a proof of origin, as specified in ''Proposed signers'' part.
- The purchase order shall be co signed by Alice Bookshop acting as a proof of receipt, as specified in ''Proposed signers'' part.
- The proof of receipt shall be counter signed by either the client or the TTP acting as a proof of acknowledgement, as specified in ''Proposed signers'' part.

Access control management:

Any purchase order successfully received by Alice Bookshop is protected by data protection laws. Only authorized personnel at Alice Bookshop may access such purchase orders; disclosure to third parties is prohibited except with the consent of the client, or in accordance with a Court order.

Dispute resolution procedures:

Any disputes arising under this policy shall be referred to a suitably qualified expert, whose decision shall be final and binding upon the parties, provided that this signature policy imposes the constraints under which any signature created under it shall be valid.

The dispute resolution procedure shall be carried out in a European court with appropriate responsibilities.

REFERENCES

Asokan N. Fairness in electronic commerce. Thesis, Waterloo, Ontario, Canada; 1998.

Asokan N, Schunter M, Waidner M. Optimistic protocols for fair exchange. In: Matsumoto T, editor. Proceedings of the 4th ACM conference on computer and communications security, Zurich, Switzerland; 1997. p. 7–17.

Bao F, Deng RH, Mao W. Efficient and practical fair exchange protocols with off-line TTP. In: Proceedings of the IEEE symposium on security and privacy, Oakland, California; 1998.

Berta IZ, Buttyán L, Vajda I. Mitigating the untrusted terminal problem using conditional signatures. In: Proceedings of international conference on information technology ITCC 2004. Las Vegas, NV, USA: IEEE; April 2004a.

Berta IZ, Buttyán L, Vajda I. Privacy protecting protocols for revokable signatures. In: Proceedings of the smart card research and advanced application IFIP Conference (CARDIS 2004); 2004b.

Berta IZ, Buttyán L, Vajda I. A framework for the revocation of unintended digital signatures initiated by malicious terminals. IEEE Transactions on Dependable and Secure Computing 2005;2(3).

Coffey T, Saidha P. Non-repudiation with mandatory proof of receipt. ACM SIGCOMM 1996.

Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory 1976;22:644–54.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

3-D secure protocol specification: core functions. Version 1.0.2. VISA; 2006.

EMV Integrated Circuit Card Specification for Payment Systems. Book 3: Application Specification. Version 4.1. EMVCo; 2007.

ETSI TR 102 038 v1.1.1. Tc security – electronic signatures and infrastructures (ESI). XML format for signature policies; April 2002.

ETSI TR 102 041 v1.1.1. Signatures policies report; February 2002.

ETSI TR 102 045 v1.1.1. Electronic signatures and infrastructures (ESI); Signature policy for extended business model March 2003.

ETSI TR 102 271 v1.1.1. Electronic signatures and infrastructures (ESI). ASN.1 format for signature policies; December 2003.

ETSI TS 101 733 v1.7.3. Electronic signatures and infrastructures (ESI); CMS advanced electronic signatures (CAdES) January 2007.

ETSI TS 101 903 v1.3.2. XML advanced electronic signatures (XAdES) March 2006.

IETF Draft. CMS advanced electronic signatures (CAdES), http://www.ietf.org/internet-drafts/draft-ietf-smime-cades-05.txt; September 2007.

IETF RFC 2560. Internet X.509 public key infrastructure online certificate status protocol – OCSP June 1999.

IETF RFC 3161. Internet X.509 public key infrastructure time-stamp protocol (TSP) August 2001.

IETF RFC 3280. Internet X.509 public key infrastructure. certificate and certificate revocation list (CRL) profile April 2002.

ISO 7498-2: Information processing systems – Open systems interconnection – Basic reference model – Part 2: Security architecture; 1989.

ISO/IEC 8824-1. Information technology – Abstract Syntax notation one (ASN.1): Specification of basic notation 2002.

Kremer S, Markowitch O. Optimistic non-repudiable information exchange. In: Biemond J, editor. 21st symposium on information theory in the Benelux. Wassenaar, The Netherlands: Werkgemeenschap Informatieen Communicatietheorie, Enschede; 2000. p. 139–46.

Kremer S, Markowitch O, Zhou J. An intensive survey of fair non-repudiation protocols. Computer Communications April 2002; 25:1601–21.

Lee B, Kim K. Fair exchange of digital signatures using conditional signature. In: SCIS 2002, Symposium on cryptography and information security; 2002.

Markowitch O, Kremer S. An optimistic non-repudiation protocol with transparent trusted third party. In: Information security conference 2001. Lecture notes in computer science, vol. 2200. Springer-Verlag; 2001. p. 363–78.

Okada Y, Manabe Y, Okamoto T. An optimistic fair exchange protocol and its security in the universal composability framework. International Journal of Applied Cryptography 2008;1(1):70–7.

Ray I, Ray I. Fair exchange in E-commerce. ACM SIGecom Exchange May 2002;3(2):9–17.

SET Secure Electronic Transaction (TM). Version 1.0, May 31, 1997. Book 1: Business description. Book 2: Programmer's guide. Book 3: Formal protocol definition. VISA.

Shao M-H, Wang G, Zhou J. Some common attacks against certified email protocols and the countermeasures. Computer Communications 2006;29:2759–69.

Wang G. Generic non-repudiation protocols supporting transparent off-line TTP. Journal of Computer Security 2006; 14:441–67. IOS Press.
W3C Recommendation. In: Bray T, Paoli J, Sperberg-McQueen CM, Maler E, Yergeau F, editors. Extensible markup language (XML) 1.0. 4th ed.; 16 August 2006.
W3C XML advanced electronic signatures (XAdES) http://www.w3.org/TR/XAdES/.
Yang S, Su SYW, Lam H. A non-repudiation message transfer protocol for collaborative e-commerce. International Journal of Business Process Integration and Management 2005;1(1).
Zhou J, Gollmann D. Evidence and non-repudiation. Journal of Network and Computer Applications 1997;20(3):267–81.
Zhou J, Gollmann D. A fair non-repudiation protocol. In: Proceedings of the IEEE symposium on research in security and privacy, Oakland, California; May 1996a. p. 55–61.
Zhou J, Gollmann D. Observations on non-repudiation. In: Proceeding of Asiacrypt '96, Kyongju, Korea. Lecture notes in computer science, vol. 1163, Advances in cryptology; November 1996b. p. 133–44.

Jorge Lopez Hernandez-Ardieta is a Ph.D. candidate in the Computer Science Department at the University Carlos III of Madrid. He currently works as a senior researcher in the private sector. His main areas of interest cover PKI, electronic signatures, non-repudiation, security in e-commerce, security standards and security evaluation methodologies. He is IEEE Member since 2008. Contact him at Avda. de la Universidad 30, 28911 – Leganés (Spain); jlopez.ha@gmail.com.

Ana Isabel Gonzalez-Tablas Ferreres is assistant professor in the Computer Science Department at University Carlos III of Madrid. Her main research interests are security and privacy for location based services and digital signature applications. She received her Ph.D. degree in Computer Science from University Carlos III of Madrid, Spain, in 2005. She is IEEE Member since 2004 and ACM Member since February 2006. Contact her at Avda. de la Universidad 30, 28911 – Leganés (Spain); aigonzal@inf.uc3m.es.

Benjamin Ramos Alvarez is assistant professor in the Computer Science Department at University Carlos III of Madrid. His research is mainly focused on non-repudiation issues of electronic signatures. He received his Ph.D. degree in Computer Science from University Carlos III of Madrid, Spain, in 1999. Contact him at Avda. de la Universidad 30, 28911 – Leganés (Spain); benja1@inf.uc3m.es.