Chapter 2
Fundamentals of Non-repudiation

Abstract This chapter gives a complete study in the state of the art about standards and elements of the non-repudiation service. It analyzes in depth the different sorts of a non-repudiation service, its participants and elements, the roles they play, the phases this service is made up of and the requirements found in each of them. Finally it reviews the existing related standards and discusses the supporting legal framework.

2.1 Specific Non-repudiation Services

Non-repudiation services help the transacting parties to settle possible disputes over whether a particular event or action has taken place in a transaction. We define a *non-repudiation protocol* as a message flow in which entities exchange digital evidence in order to provide such non-repudiation services.

In an electronic transaction, message transfer is the building block and there are two possible ways of transferring a message (see Figure 2.1).

1. The originator O sends the message to the recipient R directly; or
2. The originator O submits the message to a *delivery agent* D which then delivers the message to the recipient R.

In the direct communication model, because the originator and the recipient potentially do not trust each other, the originator is not sure that the recipient will acknowledge a message it has received. On the other hand, the recipient will only acknowledge messages it has received. In order to facilitate a fair exchange in which neither party will gain an advantage during the transaction, a TTP will usually be involved. Of course, the extent of the trusted third party's involvement varies among different protocols, and as we will see in Section 2.3, this provides for a protocol distinction.

To establish the accountability for the actions of the originator and the recipient, the following non-repudiation services are required.

J.A. Onieva et al., *Secure Multi-Party Non-Repudiation Protocols and Applications*,
DOI: 10.1007/978-0-387-75630-1_2,

- *Non-Repudiation of Origin* (**NRO**) is intended to protect against the originator's false denial of having originated the message. *Evidence of Origin* (EOO) is generated by the originator, or a TTP on its behalf, and will be held by the recipient.
- *Non-Repudiation of Receipt* (**NRR**) is intended to protect against the recipient's false denial of having received the message. *Evidence of Receipt* (EOR) is generated by the recipient, or a TTP on its behalf, and will be held by the originator.

In the indirect communication model, a *delivery agent* is involved to transfer a message from the originator to the recipient. In order to support the settlement of possible disputes between the originator and the delivery agent or between the originator and the recipient, the following non-repudiation services are required.

- *Non-Repudiation of Submission* (**NRS**) is intended to provide evidence that the originator submitted the message for delivery. *Evidence of Submission* (EOS) is generated by the delivery agent, and will be held by the originator.
- *Non-Repudiation of Delivery* (**NRD**) is intended to provide evidence that the message has been delivered to the recipient. *Evidence of Delivery* (EOD) is generated by the delivery agent, and will be held by the originator. Similarly, we should be aware that evidence provided by this service cannot be used to make further deductions about the delivery status without some sort of assumption in the communication channel.

EOS and EOD are provided by the delivery agent to the originator and could be used in two possible contexts. They could be used for resolving disputes over the service provided by the delivery agent. In this case, the delivery agent is a party to the dispute and does not act as a TTP, and EOS and EOD establish the accountability for the delivery agent's actions. On the other hand, when EOS and EOD are used outside disputes between the originator and the delivery agent, e.g. for testifying the time of submission and delivery, the delivery agent has to be a trusted third party which will not collude with the originator to provide bogus evidence. We will further discuss this and other problems in Chapter 4, in which a non-repudiation protocol with an *intermediary* or delivery agent is presented and analyzed.

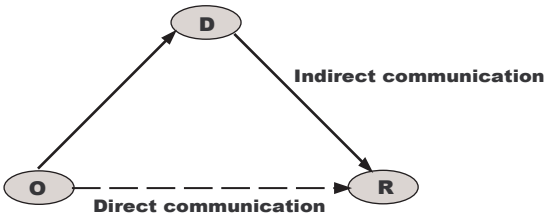

Fig. 2.1 Models of Message Transfer

2.2 Evidence

This is the data that can be used if a dispute arises. It can be either generated and stored by the local user or by a third party. Its format depends on the cryptographic mechanisms agreed in the service. Typically, examples are *digital signatures* (public key cryptography) and *secure envelopes* (secret key cryptography). Whichever the format is, this evidence has to be composed of the common information that helps to clearly identify a transaction and thus resolve a possible dispute in a more deterministic way. Some of these common elements are:

- Non-repudiation service to which evidence is related
- Non-repudiation policy identifier
- Originator identity
- Recipient identity
- Third party identity if evidence generator differs from the originator
- Message or a digital fingerprint
- Message identifier
- Information needed for verifying evidence (i.e. digital certificate, symmetric secret key info) if it is not publicly available
- TTP's identifier and role (see Section 2.3) when involved in the service
- Unique evidence identifier
- Time information (time and date that evidence was generated, expiry date, ...). If this data is certified by a *Time Stamp Authority* (TSA), it could include a timestamp service identifier.

When a secure envelope is used to provide evidence, data is stamped with a secret key known only by the TTP, thus being the generator and verifier of evidence as requested by the users.

TTP participation can be relaxed through the use of smartcards or manipulation-resistent modules [81] in which secret keys are properly installed. In this case, the smartcard plays the role of a distributed TTP. The smartcard of the generator is used for evidence generation and the verifier's one only for validation. The latter one cannot be used to generate evidence with the secret key (even if it is the same one), such that only the user who owns the generator smartcard could have created the evidence. This is achieved by correctly installing the secret key and the module which controls whether the user can use its smartcard for generation or verification. This module is tamper-proof and different for the generator and the verifier such that it performs just one of the two possible functions.

The secure envelope maintains confidentiality (e.g. symmetric cipher with the secret key) and integrity of the information using a digital fingerprint (i.e. hash function).

When a digital signature is used to provide evidence, information is enclosed in a data structure digitally signed such that only the generator can sign the data and the rest of participants (recipients and TTP) can verify it. Unforgeable digital signatures

provide a clear statement of the essential components of handwritten signatures; namely, a user's ability to sign by itself, a universally agreed verification procedure and the assertion that it is unfeasible (or at least very hard) to selectively forge signatures in a manner that passes the verification process without being detected.

In order to bring all of this into reality, digital signatures used as evidence in a non-repudiation service need an infrastructure backing it up. As we mentioned in Section 2.3, there will be a third party certifying participants' link between their identity and public key. Only in this way any recipient can verify the digital signature. Digital signatures introduce a new disrupting element in the non-repudiation service, as the link certified by the TTP (often referred as digital certificate) may have an expiry date. This fact has to be checked when evidence is verified either by the recipient or a TTP (e.g. an adjudicator). If this link has expired, evidence will be valid only if it was generated before. For this reason, time information has to be included in the evidence generated.

In general, it is more efficient, in terms of computation, for users to use secure envelopes with symmetric techniques. Nevertheless, in this case:

a) Principals have to **unconditionally trust** a third party for evidence generation and verification;
b) TTP's on-line availability is needed in order to provide the service when requested;
c) If users are to relax the TTP participation as stated previously, then they need to use dedicated hardware to avoid the TTP being a bottleneck.

So, users would likely prefer to use digital signatures because:

a) There is an **implicit trust** over the TTP computing the digital certificates and an implicit cost derived from the continuous revocation info update needed (see Section 2.3 for further reference), but this trust can be relaxed with legal agreements between users and authorities, audited registration processes and a quite advanced standardization [80];
b) **Trust** imposed over the TTP is **less critical** than in the former case, since the TTP certifies the existence of a binding between a user and a public key, verifying at the same time that this uniquely corresponds to a private key. But this TTP does not need to know the key itself. So, there is no danger of this entity accessing the content or even being able to generate it (as with secure envelopes).

Additionally, Maurer [100] proposed a novel view of digital evidence called *digital declarations*, based on a digital recording of a willful act indicating agreement to a document or contract. This proposal tries to address some of the problems related to digital signatures as mentioned above. It also includes new elements in the digital evidence (like willful acts) to augment the concept of evidence, bringing it nearer to the one used in human judgements. Among all the concepts introduced by Maurer, the semantic of certificates is very important. He proposes that when registering the public key, the user must explicitly commit to be liable for signatures with respect to that public key. Evidence confirming this commitment, designated

as *commitment declaration*, is generated and stored by the *Certification Authority* (CA) and can be presented by it if the need arises. This simple change has several important implications.

- The certificate has absolutely no value as evidence in court, only the commitment declaration does.
- Only the recipient of a signature (evidence) must trust the CA.
- An expiration date stated on the commitment declaration must be interpreted differently. It specifies until when evidence can be presented as valid, regardless of when it was generated. In other words, evidence expires, not public keys. As a consequence of this view, the validity period of evidence should be kept short.
- A commitment declaration cannot be revoked. Revocation of a public key is impossible (not needed).

Actually, with these definitions, the signature seems to be more insecure than in the traditional view when revocation is possible while the commitment declaration is valid. But, on the other hand, it seems to be closer to the business model if we consider the discussed users' liability in the traditional approach [1]. Maurer proposes the concept of delegation signatures (digital signatures assisted by TTPs) to strengthen its security. Furthermore, this digital declaration and commitments are a new approach to digital evidence with no implications on how non-repudiation protocols handle the evidence.

2.3 Roles of the TTP

One of the main features which allows us to classify the TTPs is its role in a non-repudiation service. A TTP which does not participate actively in the non-repudiation service; i.e., it will be invoked only when there is something wrong in a transaction, is referred to as an *off-line TTP*. An *on-line TTP* participates in the generation and verification of evidence throughout the protocol instance. An *in-line TTP* acts as an intermediary in all the interactions among the users. The difference between third parties that are used only in case of exceptions and third parties that are actively involved in a protocol was first explained in [47]. Obviously, the first type is preferred if efficiency is the major concern, but in some situations and e-commerce applications, to have a delivery agent or intermediary could be the best practical solution.

Other roles have appeared as a consequence of research achieved in exchange protocols. These new approaches aim at eliminating the involvement of the TTP completely but need strong requirements; either all involved parties must have the

[1] In the current digital signature laws, the "hot potato" does not come from the technical aspects but from the users' liability when it does not understand the technical process or this is done without its knowledge.

same computational power as in *gradual exchange* or fairness depends on the number of protocol rounds [97] as in *probabilistic protocols*.

At the same time there are additional TTPs which provide services needed by the non-repudiation service.

- *Certification Authority* – It provides authentication information. This information will be needed for authentication purposes (e.g. prior to the beginning of the protocol), binding a public key to an identity as described in ITU X-509 Recommendation [80] for digital certificates. It allows to digitally sign messages as well as their verification. It also provides frequent revocation information of these certificates, since if a user accepts a revoked certificate as valid, all security services based on digital certificates can be bypassed. In summary, it provides the needed infrastructure for digital signatures and authentication.
- *Time-Stamp Authority* – The time that in which event occurs can be as important for the e-commerce application as whether it took place or not. It can be used for *QoS* purposes (e.g. to see whether the delivery agent fulfilled its promise to deliver the message in a timely way), or just because it is needed for the dispute resolution process. Since digital signatures can be revoked, it is important to specify the time (slot) in which the signature was generated [69, 99, 131]. If it was generated prior to the revocation of the certificate, then evidence has to remain valid, at least, till its expiration (defined by the non-repudiation policy in effect). This time could be provided by the originator of the evidence. Nevertheless, if it is one of the principals participating in the protocol, as trust is not often assumed among their clocks, then a TTP has to do this task. This entity is the TSA, which includes a time-stamp to evidence and encloses it in a way that maintains its integrity and authentication information (e.g. digital signature).
- *Electronic Notary* – A notary is trusted by the entities to provide correct evidence on their behalf or verify evidence correctly as well as for registering it [93]. A registration token can be provided to the entities such that they can access and refer to the evidence using the audited information. This audited information can be composed by time, identities of the parties involved, a digital fingerprint of the message and non-repudiation policy used. In practice, a TTP acting in-line or on-line in the protocol can notarize the evidence.
- *Adjudicator* – This is the party which drives the dispute resolution process to a conclusion depending on evidence presented by the entities and optionally contacting participating entities. In order to facilitate its task, a well defined dispute resolution process in accordance with the non-repudiation policy must exist. This dispute resolution process has to take into consideration the legal framework in which it is defined. New or established ODR processes can be used [41].

2.4 Non-repudiation Phases

Non-repudiation services establish accountability of an entity related to a particular event or action to support dispute resolution. Provision of these services can be divided into different phases such as: evidence generation, evidence transfer, evidence verification, evidence storage, and dispute resolution.

Evidence Generation

Evidence generation is the first phase in the provision of a non-repudiation service. Depending on the non-repudiation service being provided and the non-repudiation protocol being used, evidence could be generated by the originator, the recipient, and/or the TTP. The elements of non-repudiation evidence and the algorithms used for evidence generation are determined by the non-repudiation policy in effect. When non-repudiation of origin and receipt services are required, evidence of origin and receipt are usually generated by the originator and the recipient, respectively, if digital signature is used for evidence generation. When non-repudiation of submission and delivery services are required, evidence of submission and delivery will be generated by a TTP like a notary or a delivery authority. If a secure envelope is used for evidence generation, it should always be generated by a TTP on behalf of the originator or recipient.

A TTP may also generate and provide supporting evidence in a non-repudiation service. For example, in a fair non-repudiation protocol [132], the notary will digitally sign the message key provided by the originator and make the confirmed message key available to both the originator and the recipient. The confirmed message key will serve as part of non-repudiation evidence to prove that the message key was sent from the originator (via the notary), and is available to the recipient.

Evidence Transfer

Evidence transfer is the most challenging phase in the provision of a fair non-repudiation service. It mainly consists of the sending and reception of evidence among participants. Actually, it represents the core of a non-repudiation protocol. It is greatly influenced by communication channel properties. The different options are as follows:

1. The communication channel is *unreliable*. In this case, data can be lost.
2. The communication channel is *resilient* (also called asynchronous network). In this case, data is delivered after a finite but unknown amount of time.
3. The communication channel is *operational* (also called synchronous network). In this case, data is delivered after a known, constant amount of time.

An unreliable channel will in most cases be transformed into a resilient channel by the use of an appropriate transport protocol (e.g. retransmissions).

Evidence Verification

Newly received evidence should be verified to gain confidence that the supplied evidence will indeed be adequate in the event of a dispute arising. The verification procedure is closely related to the mechanism of evidence generation.

Evidence generated through a digital signature can be verified by any party to which the public key certificate and the revocation information (e.g. the CRL or OCSP server [2]) are available. According to the requirements on non-repudiation evidence defined in Section 2.2, the origin, integrity and validity of a digital signature should be verified. In order to verify the integrity of a digital signature, the verifier needs to use the verification key to check whether the digital signature is the result applied to the expected message. For verification of the origin of the digital signature, the verifier needs to check whether the verification key is bound to the identity of the expected signer in the public key certificate. To verify the validity of the digital signature, the verifier needs to check whether the verification key had not expired and not been revoked at the time that the signature was generated. The last step implies that the verifier needs to check:

1. the trusted time stamp which is applied on the digital signature to identify the time of signature generation;
2. the expiration date of the verification key specified in the public key certificate;
3. the revocation information of the public key certificate.

If evidence is generated through a secure envelope, it should be verified by a trusted third party at the request of the user because the secret key for evidence generation and verification is only held by the TTP. Obviously, the extra communication between the user and the TTP will cause a substantial delay which might be unacceptable for many on-line electronic transactions.

Evidence Storage

Because the loss of evidence could result in the loss of future possible dispute resolution, the verified evidence needs to be stored safely. The duration of storage will be defined in the non-repudiation policy. For extremely important evidence aimed at long term non-repudiation, it could be deposited with a TTP.

There are different associations and organizations for long term archives like ARMA [8] and ERA [18], and this is an active research and development area [111]. It is specially important to mention the IETF Working Group Long-Term Archive and Notary Services (LTANS) [14] since non-repudiation of access to documents is one of the design principles. The objective of the LTANS working group is to define requirements, data structures and protocols for the secure usage of the necessary

[2] Certificate Revocation List (CRL) is a data structure which maintains reference to all the revoked certificates. On-line Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

archive and notary services. Up to date, the Long-Term Archive Service Requirements [125] and Evidence Record Syntax [63] have been published as RFCs.

Dispute Resolution

Dispute resolution is the last phase in a non-repudiation service. This phase will not be activated unless disputes related to a transaction arise. When a dispute arises, an adjudicator will be invoked to settle the dispute according to the non-repudiation evidence provided by the disputing parties and the non-repudiation policy in effect. This policy should be agreed in advance by the parties involved in the service.

The adjudicator needs to verify the evidence, probably with the assistance from other TTPs, e.g. from a notary when evidence was generated through a secure envelope. Nowadays, different on-line arbitrator platforms [3] exist which allows for dispute resolution processes through document and evidence transactions as well as the cooperation of on-line parties [49, 9]. The dispute resolution process can either be registered in one of these platforms and use its services or use its own rules for the definition of an on-line arbitrator.

2.5 Non-repudiation Requirements

Different targets of each non-repudiation service may influence the protocol design. Nevertheless, there are several common requirements on the design of a good non-repudiation protocol:

- *Fairness*: Repudiation can only be prevented when each party is in possession of proper evidence and no party is in an advantageous position during a transaction. The reliability of communication channels affects evidence transfer. Moreover, a dishonest party may abort a transaction, which could leave another party without evidence. Various fair non-repudiation protocols with different features have been proposed. Some of them can be found in [90].

  Asokan defined two levels of fairness [23]. A protocol fulfills *strong fairness* when the exchange is completed, the sender A can prove to an arbitrator that the recipient B has received (or can still receive) the item, without any further intervention from A. On the other hand, a protocol fulfills *weak fairness* when the exchange is completed, A can prove to an arbitrator that B has received (or can still receive) the item, or otherwise an affidavit can be presented to demonstrate that B misbehaved or a network failure occurred.

- *Efficiency* is another criteria. TTPs will usually be involved in non-repudiation services and its involvement will be essential in order to determine the efficiency of the protocol. Fair non-repudiation protocols proposed in [28, 27, 133, 112, 24,

[3] Note that these platforms themselves may need to implement a non-repudiation service.

98, 102] meet the criteria of efficiency and are often called *optimistic* protocols. Some authors define this property as *effectiveness*; that is, if no error occurs and no party misbehaves, then the TTP should not intervene.

- *Timeliness* is also desirable in evidence transfer. For various reasons, a transaction may be delayed or terminated. Hence, the transacting parties may not know the final status of a transaction on time, and would like to unilaterally bring a transaction to completion in a finite amount of time without losing fairness.
- *Policy* has to perfectly define all the parameters needed by the non-repudiation service, some of which can be: rules for evidence generation and verification, rules for evidence storage, evidence use and the dispute resolution process. More specific parameters to be defined by the non-repudiation policy in effect are identified throughout this chapter as, for instance, the algorithms needed for evidence generation and verification.

  In [129], a general criteria is presented as a set of questions that can be used as a guideline. Here, we refine this set with more questions that should be addressed by the non-repudiation policy.

  Related to evidence generation:

  - What evidence should be generated in the non-repudiation service?
  - Which TTP should be involved in evidence generation?
  - What elements should be included in the evidence?
  - Are all of them mandatory?
  - Which cryptographic algorithms will be used?
  - What is the encoding format?
  - What is the length of cryptographic keys?
  - Which parties will be involved in the generation process?

  Related to evidence transfer:

  - Which non-repudiation protocol will be used?
  - Which TTP will be involved in evidence transfer?
  - What are the channel assumptions?

  Related to evidence verification and storage:

  - What mechanism will be used for maintaining the validity of evidence?
  - Which TTP will be involved in evidence verification?
  - How long should the evidence be stored?
  - Which cryptographic algorithms will be used for verification?
  - Under which circumstances is the evidence regarded as valid?
  - Does the evidence need to be confidential?
  - What are the access control rules for accessing the evidence?

  Related to dispute resolution:

- Which entity will play the role of adjudicator?
- Which parties should be involved in dispute resolution? And which TTP?
- What evidence should be provided?
- What are the rules and steps followed in the resolution process itself?
- What is the expiry date of evidence?
- Which law should be referred to enforce the arbitration?

All of these requirements will be further discussed and used as guidelines on the design and analysis of the different multi-party non-repudiation protocols developed in this book. Nevertheless, there are optional requirements depending on the application itself. If the application requires them, they turn out to be as critical as the common ones previously defined. These optional requirements are as follows.

- *Verifiability of TTP* – This property adds one level of security to the protocol itself when it does not exist a strong trust relationship among participants with the TTP which collaborates in the protocol. If the TTP misbehaves resulting in a loss of fairness for any participating entity, all harmed parties will be able to prove it to an arbitrator or verifier. It can be very useful during the initial setup of a non-repudiation infrastructure as well as in those scenarios in which the TTP has to be selected by the entities on the fly (e.g. in an ad-hoc network). It usually assumes that when the TTP misbehaves, the rest of the entities are honest.
- *Transparency of TTP* – It also appears in the literature as *invisible TTP*. If the TTP is contacted to help in the protocol, the resulting evidence will be the same as the one obtained in the case the TTP is not involved. This is especially important in practical cases, in which an institution does not wish to change the existing processes to accommodate the new signatures or affidavits generated by TTPs. At the same time, this property helps on the privacy of users with respect to the use or not of a TTP during the protocol run.

Unfortunately, these last two properties are more often incompatible (achieving one of them increases the difficulty to fulfill the other one) and a trade-off has to be assumed when designing the protocols.

2.6 Analysis of Standards

The ISO and ITU standards provide a guideline for engineering and should reflect the state-of-the-art of science and technology. Non-repudiation is one of the security services in the ISO/OSI security framework, and is especially important for securing electronic commerce. Many efforts have been devoted to the standardization of non-repudiation services and mechanisms. However, some issues have not yet been well addressed.

There are two international standards dealing with non-repudiation: ISO/IEC 10181-4 [73] [4] and ISO/IEC 13888 [76, 75, 74]. ISO/IEC 10181-4 refines and extends the concept of non-repudiation services as described in ISO 7498-2 and provides a framework for the development and provision of these services. In this framework, the goal of non-repudiation and types of non-repudiation services are defined. The basic mechanisms for non-repudiation services and general management requirements for these services are identified. The roles that a TTP plays in non-repudiation services are listed. The relationship of non-repudiation services to other security services is explained. As a general framework, this standard does not include specific non-repudiation mechanisms. This remains as an open issue treated in [75, 74].

ISO/IEC 13888 "Information technology - Security techniques - Non-repudiation" is composed of three parts. ISO 13888-1 [76] [5] serves as a general model for subsequent parts specifying non-repudiation mechanisms using cryptographic techniques. It establishes two main types of evidence, the nature of which depends on cryptographic techniques employed: the *secure envelopes* generated by an evidence-generating authority using symmetric cryptographic techniques, and *digital signatures* generated by an evidence generator (which can be the user itself) or an evidence generating authority using asymmetric cryptographic techniques. It also describes non-repudiation mechanisms generic to the various non-repudiation services for the following phases of non-repudiation (see Section 2.4): evidence generation, transfer, verification, storage and retrieval, and dispute resolution. Those mechanisms are then applied to a selection of specific non-repudiation services (see Section 2.1) such as non-repudiation of origin, non-repudiation of delivery, non-repudiation of submission, and non-repudiation of transport. The standard also recommends how a smartcard (which is called a manipulation-resistent module) can be used to generate, store and validate evidence.

In ISO 13888-2 and ISO 13888-3 [75, 74], a set of non-repudiation mechanisms based on symmetric and asymmetric cryptographic techniques are identified. All of them are final international standards in the different phases that ISO/IEC apply to its documents. The history of this multipart standard which is being developed by ISO/IEC JTC1/SC27 dates back to August 1991 [72]. Zhou's book [129] analyzes the ISO/IEC 13888 non-repudiation mechanisms, and points out their weaknesses and limitations. It also discusses the problems on defining the roles of time stamps in the ISO/IEC 13888 non-repudiation evidence.

In 2006, in response to a request of ISO Subcommittee 27 (SC27) Secretariat, the Working Group 2 (WG2) of SC27 agreed to revise ISO/IEC 13888-2 as well as ISO/IEC 13888-3. The same happened later with ISO/IEC 13888-1. Drafts of the three parts have been circulated within WG2, but no final documents are available yet, though up to the moment it seems that changes will not be dramatic.

On the other side, ITU defines a general framework for the provision of non-repudiation services in X.813 [81] similar to ISO/IEC 10181-4. It defines non-

[4] It has been revised by 10181-4:1997 Information technology – Open systems interconnection – Security frameworks for open systems: Non-repudiation framework.

[5] This document revises ISO/IEC 13888-1:1997, which is withdrawn.

repudiation as "the ability to prevent entities from denying later that they performed an action". The Non-repudiation Framework extends the concepts of non-repudiation security services as described in X.800 and provides a framework for the development of these services. It also identifies possible mechanisms to support these services and general management requirements for non-repudiation.

2.7 Supporting Legal Framework

When non-repudiation services are enforced in e-commerce, its legal framework should be considered. The legal framework of e-commerce has been traditionally provided by governments in order to foster the growth of the digital economy, giving customers and companies greater confidence in their on-line transactions. This legal framework has been focused on the lawfulness of e-commerce transactions, such as evidence collection in order to protect different participants.

In December 1999, the European Union (EU) approved a Directive [52] giving digital signatures on contracts agreed upon over the Internet the same legal status as their handwritten equivalents. This was regarded as a crucial step in the struggle to put Europe ahead in electronic commerce. However, this Directive is not exempt from difficulties [48].

As a sample, in Spain, the *Real Decreto 14/1999* (September 17th) gave a first step towards regulation of digital signatures. A complete review with inclusion of digital national IDs and total renewed equivalence between digital signature and hand-written signature appeared in the Law 59/2003 of Digital Signature (December 19th). The new equivalence introduces the concept of "acknowledged digital signature" as the one generated using acknowledged digital certificates and secure ciphering devices, allowing at the same time to unify this type of certificates for QES among the countries of the EU. Nevertheless, any digital signature will be regarded as legal evidence (conclusive or not). This law seems to be quite important whenever the type of evidence has to be decided, since it is stated that

> The digital signature constitutes an instrument which is able to check the origin and integrity of messages, offering the foundation for avoiding repudiation if time-stamps are used.
>
> Art. 8 – The support in which the electronic data appears digitally signed is legitimate as documental evidence in a judgement.

So, it is clearly described that in case that disputes have to be resolved by an official judge, digital signatures will be more likely regarded as evidence than its counterpart secure envelope for the Spanish law and, in general, for the European one.

Nevertheless, as we have seen for the European Directive on Electronic Signatures, treatment of digital evidence from a legal point of view is not trivial, and there is a very interesting discussion in [100] about legal issues of evidence. Despite of the efforts from governments on bringing digital signatures for non-repudiation services into law, there is still a lack of internationally applicable law, lack of viable

business models for fostering the creation of a global PKI, problems with the integration into business processes and the abstractness and complexity of the subject matter resulting in slow user acceptance.

As stated in different laws, digital signatures will have to be treated as handwritten ones are. Actually, the value of handwritten signatures is not their security (indeed, they are easy to forge), but rather that it creates a situation in which a person knows whether or not she signed, thus guaranteeing her awareness of performing a conscious and wilful act. Due to this guaranteed awareness, the denial of having signed a document is a precise and meaningful claim, equivalent to the serious claim that the signature is forged. Whether it happens with digital signatures is a crucial issue in the legal framework accepting digital evidence.

We assume (it is stated so in most laws for e-commerce) that digital evidence (e.g. digital signature) alone implies liability. However, legislators have recognized the problem that if only digital signatures were relevant in a dispute, then users would have no possibility to defend themselves in presence of a correct digital signature. This raises the question of whether the presence of a digital signature involves a willful act from the alleged creator. In other words, it must be solved when electronic evidence is regarded as *documentary evidence* [115] - whether it is expected to 'stand on its own' and requires no context or interpretation by expert witnesses, or it is just electronic evidence as supporting evidence (where independent explanation of its relevance is necessary). Basically, it consists of finding an intersection between digital evidence and willful act. Two possible solutions can be found.

1. A digitally recording of a willful act (e.g. a video recording of the user clicking 'OK' in its digital signature generation application over the intended digital document) is included in the digital evidence.
2. The digital signature systems ensure that there is no way in which a digital signature can be generated without the user knowledge and consent.

From both solutions, the latter one has usually been used by law. Law generally expects a highly secure system for digitally signing documents will be available (and even bring into law general features about them, as in the EU Directive). The other solution is also contemplated by law in some cases in which the presence of witnesses or additional handwritten signatures are needed. At the same time, both of them have their disadvantages. Digitally recording a willful act and transmitting it over the network to the recipient could rise some practical problems. Equally, the use of highly secure systems (and highly 'digitally' educated users), which ensures that only the user can consciously digitally sign a document is far from reality.

From the above paragraphs, a notion of *admissibility* of electronic evidence can be extracted: evidence must have been lawfully collected, it must be collected in accordance with formal requirements and must respect privacy. The crucial point is that integrity and authenticity of material should be established in court. This requires standard techniques and methods for the collection, preservation and presentation of stored material. At the same time, digital material that is not readily admissible as documentary evidence (e.g. sound and image files) may require some

form of presentation technique or technology and other supporting documentation to explain its relevance.

The key issue which summarizes the discussion above is the slight difference existing between the definitions of **Cryptographic** non-repudiation (the one considered in previous sections) and **Law** non-repudiation (the traditional view of this term as defined by laws). There are several subtle but important divergences.

1. When using the digital signature as evidence, the crypto definition does not consider the gap existing between the user's will to sign a document and the layers of hardware and software placed in the device which finally performs the mathematical and computational process of signing a digital document. In the law definition this gap cannot exist as the evidence must be generated with the physical presence and will of the user.
2. There is a shift in the responsibility of proving the signature link to a user. In the ITU definition (crypto-based), non-repudiation of origin, for instance, means the originator being unable to deny its participation in the transmission. In case of a dispute, it may need to demonstrate the evidence (e.g. digital signature) was not generated by him or the signatory has no right to repudiate a digital signature at all. On the other side, in the traditional law definition, if the alleged signatory disputes the signature as belonging to him or her then the onus falls upon the relying party to prove that the signature is in fact that of the alleged signatory.

Whether only a digital signature itself can be regarded as evidence in court or additional components (e.g. a willful act of agreement digitally recorded with respect to the document signed) are needed, remains negligible for the application of non-repudiation protocols, which includes not only the type of evidence, but also other phases as generation, distribution, validity, storage and dispute resolution.