

Non Repudiation:

Gap between Legislation and Practice

G. Chondrocoukis

Department of Industrial Management and Technology
University of Piraeus

P. Lagou

Department of Industrial Management and Technology
University of Piraeus

Abstract

Legislation does not always succeed in reflecting effectively real world conditions and addressing its requirements and needs. The scope of this paper is to show this gap between legislation and practice regarding the operation of digital signatures specifically supporting the non repudiation principle in electronic communication.

United States and European law will be taken into consideration. Specifically for United States, 'Utah Digital Signature Act' and for European legislation, European Directive 1999/93/EC [European Commission, 1999]. 'Utah Digital Signature Act' [Utah Digital Signature Act, 1999] was the first law which supported the current subject after which relevant legislation was adopted by several other states [Thomas J. Smedinghoff, Ruth Hill Bro of Baker & McKenzie, LLP, 1999]. Similarly, the European Directive 1999/93/EC has been adopted by European Member States and has been transferred to local legislation (in Greece, Presidential Law 150 [Presidential Law 150, 2001]). Both legislations support the operation of electronic signatures and define that this technology should be accepted for the provision of non repudiation in electronic communications.

The 'Utah Digital Signature Act' (from now on referred as US law) and the EU directive 1999/93/EC (from now on referred as EU directive) will be reviewed, analyzed, and compared in order to identify their weaknesses relating to the provision of non repudiation. Recommendations will be made on the improvement of existing legislations in combination with the technological model which they support and a new model will be presented to address the identified gaps and vulnerabilities.

Key words

Non repudiation, digital signatures, Public Key Infrastructure (PKI), Biometrics

Introduction

With technological evolution, electronic means is used more and more for communication and the conduct of transactions. The reason for this is that internet provides a convenient infrastructure which facilitates such activities: communication

through emails, chat forums, blogs, purchases through electronic commerce and many more. However, it also facilitates the conduct of unauthorized activities: disclosure of confidential information, alteration of transmitted messages or published material, and many more. These issues create problems which prohibit the use of digital communication for additional applications.

One such issue which needs to be addressed is impersonation. In electronic communication it is difficult to verify the identity of the transacting parties. That is why the provision of authentication and even more of non repudiation is essential for the proliferation of digital communication and the development of new transacting models.

1. Definition of Non Repudiation

Non repudiation is the principle which prevents individuals from denying (repudiating) their participation in a transaction. It is linked to the principle of authentication, which is identity verification, but has stronger requests regarding the produced proofs. The main difference is that in authentication, an entity is required to prove to the second transacting party their identity where in non repudiation, a third party is called to make the decision whether the transaction took place [Zhou Jianying, 1997].

Briefly described, non repudiation includes the principle of authentication, but requires the presence of strong evidence which can be used in case a third party has to determine whether a transaction or communication was conducted.

According to ISO/IEC 13888-1 [International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2004], the following principles have to be satisfied in order for a technical model to provide Non Repudiation services:

- *Creation of evidence for the participation of an entity in a transaction*
- *Collection of evidence*
- *Preservation of evidence for a time period in which they can be requested if needed*
- *Availability of evidence for a third party*
- *Verification of evidence authenticity should be possible*

These principles are necessary for the resolving of disputes regarding the conduct of a transaction or communication which took place electronically. The last requirement sets emphasis on the important role of security of the technical model which provides non repudiation principles and the need for mitigating the risk of its circumvention and exploitation.

In real world conditions, non repudiation is implemented by the use of a handwritten signature. That is why in regulations and legislations, addressing of non repudiation in electronic transactions is defined as being '*as valid as if it had been written on paper*' (US law) or as valid as a hand-written signature (EU directive).

2. US Legislation

In United States, the first law which was created to address the issue of non repudiation was Utah Digital Signature Act [Utah Digital Signature Act, 1999]. Most states after that

have formed relative legislation which has as a purpose to support the operation of digital signatures for the provision of non repudiation.

Specifically in Utah Digital Signature Act, in Code 46-3-402 ‘Effect of digital signature’, it is stated:

A digitally signed document is as valid as if it had been written on paper.

This phrase defines that the digital signature is as valid as a handwritten signature which consequently means that it legally supports the principle of non repudiation.

Most significant codes of the Utah Digital Act are briefly described:

46-3-104 Contents of a certificate -- Effective date

In this code, the minimum information/fields which should be included in a certificate are defined.

46-3-105 Licensure and qualifications of certification authorities.

This code includes the conditions under which institutions and individuals can be accepted to operate as certification authorities.

46-3-106 Performance audits and investigations.

Certification authorities’ operation will be audited and categorized according to their compliance with the current legislation. Four categories have been defined: full compliance, substantial compliance, partial compliance, non compliance.

46-3-107 Record-keeping by certification authorities.

Certification authorities reserve mainly records provided by their customers as supporting evidence of their identity.

46-3-108 Cessation of certification authority activities.

Certification authorities’ responsibilities upon cessation are defined.

46-3-109 Hazardous activities by any certification authority prohibited.

Certification authorities have a responsibility to mitigate risks towards its subscribers and the people who rely on the certificates provided.

46-3-110 Issuing a certificate

The conditions which need to be satisfied in order for a certification authority to issue a certificate are stated.

46-3-111 Representations by the subscriber accepting a certificate.

According to this section, the subscriber for whom a certificate has been issued accepts the responsibility that all information which is presented into the certificate is true.

46-3-112 Control of the private key

In this code, it is stated that the private key remains under the possession and control of the subscriber.

46-3-113 Duties of a licensed certification authority in issuing a certificate.

Certification authorities are obliged under this section to provide valid information into the issued certificates.

46-3-114 Suspension of a certificate.

Conditions, under which a certificate is suspended, are described.

46-3-115 Revocation of a certificate.

Conditions, under which a certificate is revoked, are described.

46-3-116 Expiration of a certificate.

The expiration date of a certificate is defined within the certificate.

46-3-117 Liability of a licensed certification authority.

Limitations in the liability of licensed certification authorities are defined.

46-3-118 Presumptions established by a digital signature

It defines the conditions under which the certificate acknowledges the relative digital signature.

46-3-119 Effect of digital signature

It has been stated earlier in this section, it is stated that the digital signature is as valid as the handwritten signature.

3. EU Legislation

As it has already been mentioned, the European Directive 1999/93/EC [European Commission, 1999] supports the provision of non repudiation by digital signatures. Specifically, in article 5 'Legal effects of electronic signatures', it is stated that:

'Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

- (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data'*

Therefore, the directive supports that non repudiation (...a hand-written signature satisfies those requirements in relation to paper-based data) is provided when the following three conditions are satisfied:

1. An advanced digital signature is used,
2. The advanced digital signature is based on a qualified certificate and
3. The digital signature is created by a secure-signature-creation device.

What do these mean in practice?

Advanced Digital Signature

According to the Directive (Article 2, Definitions), ‘advanced electronic signature’ means an electronic signature which meets the following requirements:

- (a) it is uniquely linked to the signatory,*
- (b) it is capable of identifying the signatory,*
- (c) it is created using means that the signatory can maintain under his sole control, and*
- (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable*

Qualified Certificate

According to the Directive (Annex I, Requirements for qualified certificates), qualified certificate must contain:

- (a) an indication that the certificate is issued as a qualified certificate,*
- (b) the identification of the certification-service-provider and the State in which it is established,*
- (c) the name of the signatory or a pseudonym, which shall be identified as such,*
- (d) provision of specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended,*
- (e) signature-verification data which correspond to signature-creation data under the control of the signatory,*
- (f) an indication of the beginning and end of the period of validity of the certificate,*
- (g) the identity code of the certificate*
- (h) the advanced electronic signature of the certification-service-provider issuing it,*
- (i) limitations on the scope of use of the certificate if applicable and*
- (j) limits on the value of transactions for which the certificate can be used, if applicable.*

Secure Signature-Creation Devices

According to the Directive (Annex III, Requirements for secure signature-creation devices), secure signature-creation devices must by appropriate technical and procedural means, ensure at the least that:

- (a) The signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured,*
- (b) The signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology,*
- (c) The signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.*

4. US Law versus EU Law

The two legislations have several differences, even though they incorporate the same issue. These differences have an impact on the way they address non repudiation. The most significant differences which have been identified are the following:

1. **Statement of non repudiation:** US law states: *'A digitally signed document is as valid as if it had been written on paper'*. This means that it supports the operation of digital signatures for the provision of non repudiation without defining any other conditions. Many practical issues have not been taken into consideration which may prohibit the satisfaction of non repudiation by the use of digital signatures. On the other hand, EU directive defines: *'Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device'* will provide non repudiation. Certain preconditions are required in order that digital signatures have legal effect on non repudiation principle. Still, real world conditions have not been addressed adequately but it provides stronger definition of non repudiation addressing, than US law.
2. **Content:** US law is more detailed than EU law. It describes procedures and conditions which should be applied by certification authorities to cover most possible situations. EU law is simple and brief. It defines only the conditions for the addressing of non repudiation and nothing else. US law is considered to be more successful in providing assistance and direction to certification authorities into implementing Public Key Infrastructure and consequently into addressing efficiently non repudiation.
3. **Scope:** Even though the main goal of the two legislations is to establish the operation of digital signatures, they approach this goal in different ways. US law is focused mostly on the operation of certification authorities and not so much on the digital signature. On the contrary, EU directive, defines only the legal effect of digital signatures without describing the technology or the commercial model (Public Key Infrastructure) which supports it. As pointed out previously, the description on the processes which a certification authority supports is considered a good principle for US legislation compared to EU directive, because it provides clear guidance to organizations implementing the relative technology. However, preconditions on the use of the digital signature are required as well for non repudiation implementation, which is satisfied by the EU directive but not from US law.
4. **Qualified certificates:** EU directive introduces the concept of qualified certificates and defines their use as a prerequisite for the provision of non repudiation. US law does not make any specific categorization on certificates used. As it will be analyzed, qualified certificates do not provide additional security for the provision of non repudiation and consequently their use is not considered a necessary requirement for the addressing of non repudiation.
5. **The role of an agent:** US law allows the role of an agent who acts as a representative of the owner of the digital signature during registration and issuance of the certificate. EU directive does not state that a representative can be used. The permission of a representative of the digital signature's user who will

have access to the private key increases the unauthorized disclosure risk. It is considered a weakness of US law to allow such a procedure which may violate the non repudiation principle.

6. **Possession of the private key:** EU directive states that the digital signature is created '*using means that the signatory can maintain under his sole control*'. US law states, however, that there is a possibility that the private key of the digital signature of a user can be held by the certification authority as well (and possibly by the agent as stated previously). If the private key is not only under the possession of the rightful owner, but other parties have access to it, this increases the risk of disclosure of the private key and consequently of impersonation of the digital signature's user.
7. **Audits:** Audit mechanisms are not defined in EU directive. US law defines that periodic auditing will be taking place. This is a very good practice. However, it also defines four categories of compliance for certification authorities: full compliance, substantial compliance, partial compliance, non compliance. In some cases, US law allows the exemption of certification authorities from audit obligations. Nevertheless, it does not define any differentiation regarding the provision of non repudiation considering the differences in compliance. For example, a fully compliant certification authority can provide non repudiation as well as a partial compliant? The fact that these compliance categories are not taken into account into the provision of non repudiation is considered an omission.

5. Legislation versus Real World Conditions

Legal Conditions

One of the conditions that EU directive defines is that in order to implement non repudiation, the advanced digital signature should be '*uniquely linked to the signatory*'. In theory, this is a very good hypothesis. In tangible world, this hypothesis is satisfied because the signature is created by the human entity and therefore it is uniquely linked to the signatory. However, in the digital world, the digital signature is not created by the human entity but is stored somewhere (a device, a PC, a token) and the user accesses and uses it by accessing the storage device. Therefore, the more precise description for the digital signature would be that it is uniquely linked to the signatory's PC or to a storage device rather than to the signatory. This is considered to be the main vulnerability of digital signatures regarding the provision of non repudiation and it has been identified in many papers [Carl Ellison & Bruce Schneier, 2000]. Therefore, it would be rather difficult for the second party to prove that the signatory is the only person with access to the relative digital signature if the signatory wishes to dispute it. He can claim that the storage place has been accessed by an unauthorized entity without anyone being able to prove otherwise. Consequently, conditions (b) and (c) from EU directive regarding digital signature are not very strong as well. Similarly, US law states: '*the subscriber identified in the certificate assumes a duty to exercise reasonable care in retaining control of the private key and keeping it confidential*'. Responsibility is transferred to the user but it is weak as condition for non repudiation for the same reasons which have been analyzed.

The second condition in EU directive is that the certificate is a qualified certificate. The difference between a certificate and a qualified certificate is the presence of extra fields. It is not however apparent what is the added value in the security of the digital signature that the qualified certificate provides. Why is it a prerequisite for the provision of non repudiation? What more is gained if there is a field in the digital certificate which defines the signatory's state or a pseudonym?

The secure signature creation device, which is required by EU directive but not by US law, provides a higher level of security. However, it is not considered to be sufficient for two reasons: firstly, if a digital signature is created in a secure signature device, this does not prevent it from being copied in another digital storage device as well. Secondly, it is still a device which has an access control method which can possibly be violated.

Real World Conditions

What happens in reality is not accurately reflected in the relative EU directive and US law. There are conditions which should have been taken into account, which were not identified or addressed adequately and may prevent the implementation of non repudiation.

As it has already been described, certification authorities are responsible for the issuance of digital certificates, which bind a physical entity with the digital signature. Therefore, the certification authority conducts an authentication check to verify the identity of the digital signature's legitimate owner and user. The second party in an electronic transaction relies on the certification authority and trusts that the authentication check has been performed successfully. A certification authority has been taken as an example to show how Public Key Infrastructure is implemented. This example is Adacom which is a certification authority in Greece and an affiliate company of VeriSign. For this company, the authentication check conducted depends on the usage and the class of the digital certificate. Three classes of digital certificates have been defined: Class 1, Class 2 and Class 3. The cryptographic security which is applied in all three classes of certificates is the same. The security level on a certificate is implemented by the use of a strong algorithm and the key size. However, the authentication procedure differs significantly between the three classes. The authentication procedure consists of the following:

- Class 1: The provision of an electronic address and the user name, without additional proofs of identity. These certificates are used mainly for signing emails.
- Class 2: A photocopy of the applicant's national identification card. It can be used for signing emails but also for applications with higher security requirements, like access to systems where sensitive or confidential information is stored.
- Class 3: For the issuance of a class 3 certificate, the physical presence of the applicant is required for the authentication checking. Certificates of this class can be used in similar applications as certificates of 2nd class, but with higher security requirements. They are recommended for use in transactions of high financial value.

[ADACOM, 2007]

There is no specific reference for the authentication procedure for qualified certificates and EU directive does not define any relative requirements. US law as well, even though it defines detailed procedures for other processes which are conducted by certification authorities, it briefly refers to authentication procedure. It also does not take it into

account when defining non repudiation. It defines that all digitally signed documents will be as valid as being signed on paper without requiring any preconditions on the authentication process. If the authentication checking is insufficient, as it is for class 1 and class 2 certificates, the identity of the user accessing the digital signature has not been verified and an entity can easily be impersonated. EU directive dictates that all digital signatures which are based on a qualified certificate and which have been created within secure creation devices can provide non repudiation. However, in practice, what if this certificate is qualified but authentication check is conducted as for class 1 or class 2 certificates? Is the identity of the defined owner of the certificate verified? How does legislation prevents this from taking place?

Furthermore, there is no requirement in EU directive regarding the algorithm used and the key size of the algorithm. In US law it is briefly defined that a suitable algorithm should be used but no reference on specific algorithm or standard used or the acceptable key size. The asymmetric algorithm used as well as a relatively large key size define the level of security of the digital signature and limit the possibility that attacks against the algorithm will materialize. Therefore, what happens if a digital signature (in US) or an advanced digital signature is used with a qualified certificate and is created within secure signature creation device (in EU) but the algorithm used is not strong enough or a strong algorithm is used but with a short key size? Can this digital signature provide non repudiation? If legally is defined that it does, is it technically possible to support non repudiation if it is vulnerable to cryptographic attacks? Is it not this requirement important enough to be included as a requirement in relative legislation?

Additionally, in standard RFC 3280 [Request For Comments (RFC), 2002] as well as in the previous one which was replaced by it, RFC 2459 [Request For Comments (RFC), 1999], the certificates' structure is defined as well as the structure of the Certificate Revocation List. In the structure of the certificates a field is included where the usage of the certificate is defined and is named 'Key Usage'. For this field the standard defines the following options:

- *Digital Signature*
- *Non Repudiation*
- *Key Encipherment*
- *Data Encipherment*
- *Key Agreement*
- *Key Certificate Signing (KeyCertSign)*
- *Signing of Certificate Revocation List (crlSign)*
- *Only for Encipherment (encipherOnly)*
- *Only for Decipherment (decipherOnly)*

In standard 2459 is recorded as non compatible the use of Non Repudiation and Digital Signature as key usage in the same certificate, which is however not mentioned in 3280. So how is this implemented in practice? According to US law, all digitally signed documents are as valid as being signed on paper. What if the digital certificate used does not have key usage 'non repudiation'. Is it legally binding concerning the non repudiation principle? Similarly, taking into account EU directive, an advanced digital signature which is created in a secure device and has as a 'key usage' non repudiation, even if this is not a qualified certificate, does it provide non repudiation? What if the 'key usage'

field is defined as non repudiation but the digital signature is not created in a secure device, is the statement of non repudiation use valid?

Additionally, in US law, compliance categories have been defined. These categories have not been evaluated concerning their ability to provide non repudiation. For example, what if a certification authority is partially compliant with relevant legislation; can this certification authority be considered trustworthy enough to provide digital certificates for non repudiation?

In accordance to the above statements, in a study which was published on March 2006 regarding the operation of digital signatures in Europe is recorded that digital signatures' use is limited [Commission of the European Communities, 2006]. A reason for this is that users hesitate to trust Certification Authorities. Users' trust into Certification Authorities is a basic principle for the operation of Public Key Infrastructure. Furthermore, the providers of electronic services do not support the use of this technology in the communication with their customers, being afraid of responsibilities. This proves that users do not trust digital signatures for the provision of non repudiation.

Concluding, it has been identified that legislation has not succeeded into addressing real world conditions regarding non repudiation. There are gaps which need to be considered between what is stated in the relevant EU Directive and US law and what is taking place in reality.

6. Recommended Solutions

Two solutions are recommended for the provision of non repudiation:

Improvement of current legislation

If digital signatures should be used for non repudiation purposes, relevant US legislation and EU directive should be reviewed and changes need to be made. At least the following changes should be implemented:

- There should be a condition regarding the asymmetric algorithm and the size of the key used for the creation of the digital signature as a prerequisite for the provision of non repudiation. These two factors are of major importance for the strength of the digital signature against cryptographic attacks. It is understandable that due to technological development, processing systems become faster and more intelligent within a short period of time. As a consequence, probably the defining of the use of a specific algorithm or a specific key size would not be wise because it would become obsolete quickly. However, legislation could mention that 'a strong enough algorithm should be used and a relatively long key size for the provision of non repudiation' or it could contain a reference to a widely accepted standard.
- There should be a condition regarding the authentication procedure used for the provision of the digital certificate, which binds the human entity with the digital signature. This authentication procedure should be as detailed as possible. Certification authorities should be able to verify the identity of the certificate owner for the users to trust Public Key Infrastructure for the provision of non repudiation.

- Regarding US law, only ‘fully compliant’ CAs should be able to issue certificates which provide non repudiation.
- Regarding US law, the private key should be under the possession of the digital signature’s owner and not anyone else, e.g. the certification authority or any representative. This process increases risk of impersonation and should not be allowed.
- Legal authorities should have better information on current technologies and guidance by technical consultants in order to understand relevant technological models and methods and proceed to implementation of relevant legislation as well as the ruling of cases regarding non repudiation.

Biometrics

Even if all recommended changes are implemented, there is a remaining issue relating to the use of digital signatures. A significant hypothesis has been identified, which is that the digital signature should be uniquely linked to the signatory or similarly that the private key is only used by the rightful owner. As it has already been noted, the proper way to describe the operation of digital signatures is: digital signatures are uniquely linked to a digital device which is under the signatory’s sole control. This condition is difficult to be satisfied. A technology which can satisfy this term is biometrics. Biometrics is the technology in which a part of the human body is used to verify the identity of a person.

Advantages

The use of biometrics for the provision of non repudiation has many advantages:

- The data created from a biometric are directly derived from the human entity and therefore are with no doubt ‘uniquely linked’ to the user taking part in a transaction.
- The use of biometrics is more user friendly. The user does not have to remember a secret code or hold a device where the digital signature is stored. The biometric can be provided whenever it is requested by the use of the relevant biometric reader.
- The digital certificate has a life limit of 1 year. This means that every year the user should enroll again for a new certificate. The enrolment for a biometric is only taking place once and can be used for a long period of time under normal conditions.
- The use of biometrics does not have any security requirements from the user side which makes it easier to enforce non repudiation services.

Biometric Model

The suggested model is described briefly in the following figure:

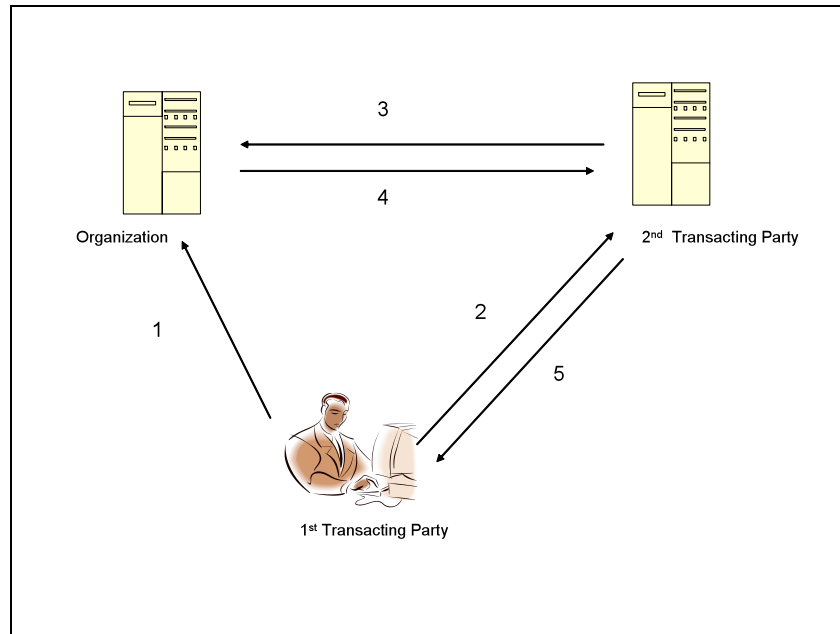


Figure 1: The Biometric Model for Non Repudiation

1. The user contacts the Organization which provides the infrastructure for the support of the biometric model. He conducts an enrollment procedure and a biometric sample is reserved in a database.
2. When the user wishes to take part in an electronic transaction in which the verification of his identity is needed he uses a biometric reader. A digital image of his biometric is sent to the second transacting party's server.
3. The second transacting party verifies the user's identity by sending the biometric received with the biometric which is kept in the organization's central database.
4. The Organization compares the biometric received with the biometric held and if they match, sends a positive reply to the second transacting party.
5. The second transacting party has verified the identity of the user and can proceed with the electronic transaction.

The suggested model satisfies non repudiation services with the hypothesis that the biometric used is strong enough that it cannot be forged. Many tests have been conducted and the biometric which is identified to be more robust is iris. Specifically, the results from 'Biometric Product Testing Final Report' which was published on March 2001 [Tony Mansfield, 2001] are represented in Figure 4:

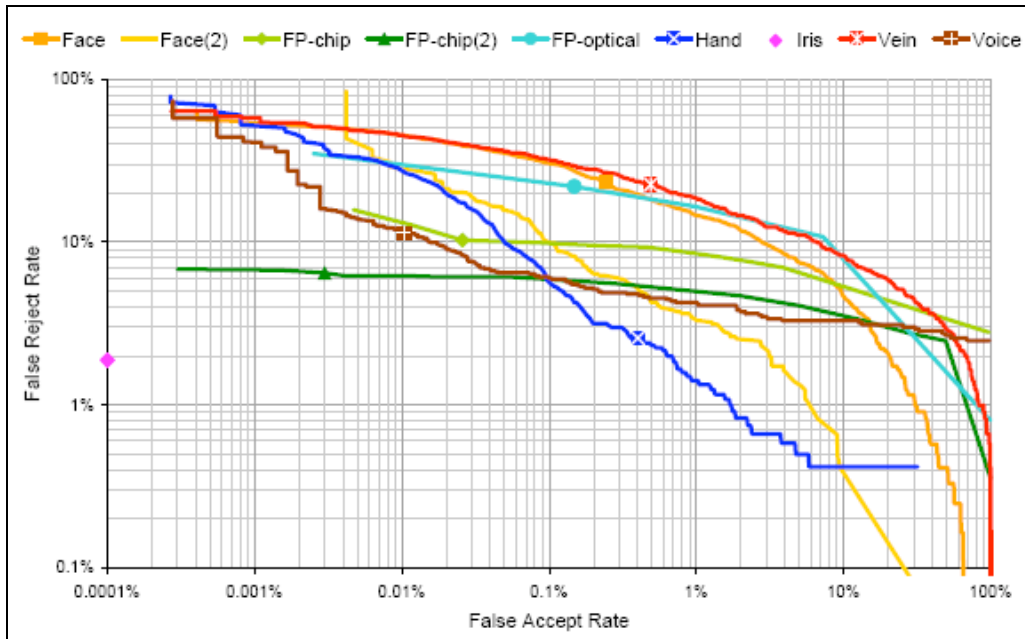


Figure 2: False Accept and False Reject Rate

It is obvious that the only biometric with False Accept Rate 0 is iris.

It is not disputed that biometric technology has drawbacks and vulnerabilities as well as the suggested model. However, it also has significant advantages comparing to other technological methods concerning the provision of non repudiation. A detailed risk analysis has been attempted from which it derives that most attacks of high and medium risk can be addressed with the implementation of relative controls [Panagiota Lagou, 2006]. Therefore, it is advised that it should be reviewed and its use regarding non repudiation services should be explored.

7. Conclusion

It has been proved that several improvement opportunities arise regarding legislation on non repudiation services. Regulators should review relative laws and take into consideration the abilities of digital signatures as well as their limits. Other technologies should be explored for the provision of non repudiation services, like biometrics. The effective implementation of non repudiation in electronic transactions will facilitate electronic commerce and can lead to the development of new applications and communication models.

8. References

ADACOM, site of ADACOM,

http://www.adacom.com/Products_Services/PKI%20%20Authentication/Client_Certificates/Class_1_2_3_Certificates.aspx 2007

Carl Ellison & Bruce Schneier, 'Ten Risks of PKI: What you 're not being told about Public Key Infrastructure', <http://www.schneier.com/paper-pki.pdf>, 2000

Commission of the European Communities, Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures
http://ec.europa.eu/information_society/europe/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf, 2006

European Commission, 1999/93/EC, http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf, 1999

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 13888-1, 2004

Panagiota Lagou, Draft PhD Thesis 'Non Repudiation with the use of biometrics', 2006
Presidential Law 150, http://www.ekt.gr/content/img/product/14911/pd150_2001.pdf, 2001

Request For Comments (RFC), RFC 2459, <http://www.ietf.org/rfc/rfc2459.txt>, 1999

Request For Comments (RFC), RFC 3280, <http://www.ietf.org/rfc/rfc3280.txt>, 2002

Thomas J. Smedinghoff, Ruth Hill Bro of Baker & McKenzie, LLP, 'Electronic Signature Legislation', <http://library.findlaw.com/1999/Jan/1/241481.html>, 1999

Tony Mansfield, Biometric Product Testing Final Report, 2001

Utah Digital Signature Act, <http://www.jus.unin.it/USERS/PASCUZZI/privcomp97-98/documento/firma/utah/udsa.html>, 1999

Zhou Jianying, 'Evidence and Non-repudiation',
<http://citeseer.ist.psu.edu/cache/papers/cs/873/http:zSzzSzhomex.s1.net.sgzSzuserzSzjyzhouzSzJNCA97.pdf/zhou97evidence.pdf> 1997