PKI Interoperability: Still an Issue? A Solution in the X.509 Realm

Ahmad Samer Wazan, Romain Laborde, François Barrere, Abdelmalek Benzekri, David W. Chadwick

PKI interoperability: Still an issue? A solution in the X.509 realm

Ahmad Samer Wazan[1], Romain Laborde[2], François Barrere[2], Abdelmalek Benzekri[2],
David W Chadwick[3]

[1]Institut Mines-Telecom/Telecom SudParis, CNRS UMR 5157 SAMOVAR,
91000 EVRY, France
samer.wazan@telecom-sudparis.eu
[2]Paul Sabatier University, IRIT UMR 5505, 31400 Toulouse, France
{laborde, barrere, benzekri}@irit.fr
[3]University of Kent, Computing Laboratory, Canterbury, Kent, CT2 7NF
d.w.chadwick@kent.ac.uk

Abstract. There exist many obstacles that slow the global adoption of public key infrastructure (PKI) technology. The PKI interoperability problem, being poorly understood, is one of the most confusing. In this paper, we clarify the PKI interoperability issue by exploring both the juridical and technical domains. We demonstrate the origin of the PKI interoperability problem by determining its root causes, the latter being legal, organizational and technical differences between countries, which mean that relying parties have no one to rely on. We explain how difficult it is to harmonize them. Finally, we propose to handle the interoperability problem from the trust management point of view, by introducing the role of a trust broker which is in charge of helping relying parties make informed decisions about X.509 certificates.

Keywords: PKI, X.509, Trust, Interoperability.

1 Introduction

While the potential of PKIs is high, this technology continues to suffer from many problems that slow its global adoption. In 2003, the OASIS technical committee investigated the reasons that prevent the widespread adoption of PKI technology. The major results of this survey [1] are:

- Poor PKIs interoperability;
- Too much legal work required;
- Hard for end users to use;
- PKI poorly understood.

Although this survey was undertaken in 2003, the issues related to interoperability, complexity of legal work and the difficulty of use by end users are still accurate and still cause severe problems.

These issues are not mutually exclusive; they are highly related to each other. The interoperability problem is the most difficult one, because it is the most complex and confusing. Peter Smith has highlighted the complexity of PKI interoperability [2]: "*[PKI] interoperability is something of a will-o'-the-wisp. You think you understand what people mean by it, and then quickly realize that you don't. In my experience, it's possible when discussing interoperability to be at cross-purposes for all of the time}". If such a group of experts has difficulties to cope with this issue, how can we imagine an unskilled person can perform this task? Today, users of certificates, and in particular relying parties, are left on their own to face this problem*".

In this paper, we open Pandora's Box by trying to explain the reasons for the interoperability problem in the field of PKIs. We show that the problem cannot be solved by defining harmonized juridical, organizational and technical rules, especially because of the cultural/juridical differences between countries. Thus, PKIs today are isolated islands; each PKI seeks to comply only with the requirements of the jurisdiction where their root CA premises are located.

Although explaining the PKI interoperability issue is the main objective of this paper, our research is also aimed at resolving this problem from a trust management point of view. Our proposed solution is also briefly presented. Our trust management based approach requires defining a new role, the trust broker, which will help relying parties to evaluate the risks and to take informed decisions about using the certificates of remote users, which they have obtained.

The rest of the paper is structured as follows. Section 2 explains what exactly a public key infrastructure is. It presents the main involved entities and PKI deployment models. In section 3, we illustrate the problem of PKI interoperability and show how it is difficult to solve the problem by defining harmonized juridical and technical rules between countries. In section 4, we present our proposition that consists in handling the interoperability problem from a trust management point of view. We also briefly present our proposal to define a new trusted third party, the trust broker, and we demonstrate the feasibility of our proposal. Finally, in section 5 we present our conclusions.

2 What is a public key infrastructure?

Many definitions of a PKI exist. The American Bar Association (ABA) defines a PKI as: "*The sum total of the hardware, software, people, processes, and policies that, together, using the technology of asymmetric cryptography, facilitate the creation of a verifiable association between a public key (the public component of an asymmetric key pair) and the identity (and/or other attributes) of the holder of the corresponding private key (the private component of that pair), for uses such as authenticating the identity of a specific entity, ensuring the integrity of information, providing support for non repudiation, and establishing an encrypted communications section*".

Thus, a PKI is not only a set of computers used for generating the key pairs and the associated certificates. It is also the set of policies, processes and people responsible for a certificate's life cycle management. The certification authority (CA), which asserts the correctness of the certificate information by appending its signature on the certificate, is the main entity of this infrastructure.

A PKI is based on a trust model described by the X.509 standard (**Fig. 1**). The model is composed of three entities: the certification authority (CA), the certificate holder and the relying party (RP). The CA plays the role of trusted third party by guarantying the correctness of the certificate information to the RP. Thus, the CA trusts the certificate holder and so issues it with a public key certificate. The relying party trusts the CA for the validity of the certificate's information. Consequently the relying party can indirectly trust the certificate holder for the current transaction.

According to RFC 5280, which defines an X.509 certificate profile for the Internet, an RP has the obligation to review the CA policy documents before accepting a certificate. It declares: "*A certificate user should review the certificate policy generated by the certification authority (CA) before relying on the authentication or non-repudiation services associated with the public key in a particular certificate*".

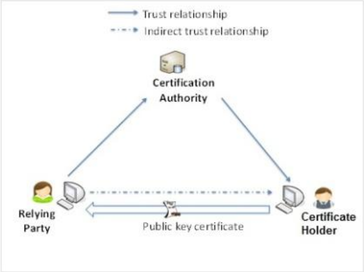

Fig. 1. X.509 trust model

To respect this obligation an RP must typically read two documents: the Certificate Policy (CP) and the Certification Practice Statement (CPS) documents. The CP document defines the application domain of a certificate and the security requirements to be realized by the CA. The CPS document defines how the CA has implemented the security requirements. It must be fairly obvious to anyone that this is a ludicrous requirement to place on most computer users.

Two different deployment models can be distinguished for PKIs: the ***closed*** and the ***open*** models. The closed model is usually applied to contexts with limited scope such as a collaboration between organizations where each organization manages its own PKI including one or more CAs. All the relationships between all the entities (RPs, CAs and certificates holders) participating in the collaboration are clarified through agreed contracts between the involved organizations.

In the open model, the relationship between a CA and certificate holders is also clarified by contracts. But, there is no such explicit contractual relationship between the CA and the relying parties (RPs). Therefore, the regulation of the relationships between a CA and the RPs is defined in legislative and regulatory frameworks rather than contracts. However, the lack of consensus between countries about the implementation of these frameworks or the way that PKIs should be regulated has given rise to the problem of interoperability between PKIs in this open model.

3 The PKI interoperability obstacle

Generally, two kinds of regulations can be identified: economic regulations and social regulations [3]. The objective of the economic regulations is to increase economic efficiency by reducing barriers to competition and innovation, often by deregulation. The objective of the social regulations is to protect the public interests such as health, safety and the environment. Thus economic interests come as secondary concern to the social regulations.

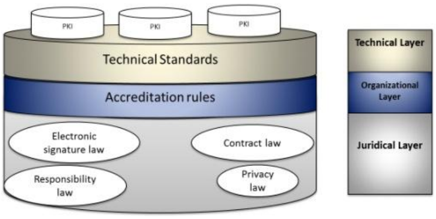

Fig. 2. Regulation layers

A PKI depends on three layers of regulations: juridical, organizational and technical (**Fig. 2**). PKI interoperability requires compatibility at these three layers. Currently, profound differences still exist between countries at each layer: juridical, organizational and technical. In the following sections, we try to interpret what the interoperability problem actually means by exposing the juridical, organizational and technical differences that exist between countries.

3.1 Juridical differences

The implementation of a PKI requires the processing of different legal issues: how to recognize electronic signatures, the validity of electronic contracts, the legal responsibilities of the involved entities (CAs, certificate holders and RPs) and the privacy rules.

Generally, the legal differences that exist today come from the different legal traditions that have evolved and are now being followed in the different countries. There are mainly two different traditions: the common-law tradition that relies on legal precedent to assess legal affairs, and the civil-law tradition that relies on the existence of laws rather than decisions of courts to assess legal affairs [4]. Consequently countries have treated all the legal issues related to PKIs according to their different legal traditions.

Differences concerning the legal recognition of electronic signatures. Three different approaches exist for validating electronic signatures: (a) the minimalist approach; (b) the technology-specific approach and (c) the two-tiered approach [6].

The minimalist approach is based on the principle of technological neutrality, which gives a minimum legal effect to all technologies. The principle of technological neutrality ensures that the legislation remains valid even when the technologies be-come obsolete. This approach is often applied in common law countries such as the US, UK and Australia. Under this approach, electronic signatures are equivalent to handwritten signatures if they fulfill certain functions. In case of dispute, the validity of electronic signatures is established a posteriori by a judge, or by a public authority [5].

In **the technology specific-approach**, laws favor one form of electronic signature; usually digital signatures. In this case, laws specify technical, juridical and financial requirements imposed on CAs in order to validate electronic signatures generated by their certificates. The disadvantage of this approach is that it makes uncertain the legal status of other types of electronic signature. The Utah State was the first to adopt such a law in 1995.

The two-tiered approach combines the advantages of both previous approaches. It is often followed in countries whose tradition is civil-law. It provides a balance between flexibility and certainty by setting minimum requirements for all types of electronic signatures and at the same time by defining a clear legal effect for certain forms of electronic signature that meet specific technical requirements. The European Union has adopted this approach through its directive 1999/93/EC on electronic signatures.

Differences about the legal validity of electronic contracts. There are two types of electronic contract: contract at a click "*clickwrap contract*" and contract at navigation "*browsewrap contract*". A "*clickwrap contract*" is a contract to which a consumer must agree by clicking the icon "I agree" before completing the transaction. A *browsewrap* contract, which is often accessible using links labeled "Legal" or "Terms of Use", is so named because such agreements state that a web site user is bound simply by "browsing" the web site [8]. In other words, the term *browsewrap* refers to any contract not requiring an explicit manifestation of assent.

Electronic contracts, whether they are *browsewrap* or *clickwrap*, are both considered a contract of adhesion. These contracts do not allow for negotiation; they are based on the principle "take it or leave it" where one party is restricted to accept all the terms prepared by the other powerful party. These contracts usually raise questions about the fairness to the weaker party.

Countries like the US tend to regularize electronic contracts mainly based on only the traditional laws of contracts, whilst other countries like those in Europe, add different extensions to the traditional laws of contracts [7]. By consulting case law handled until 30-06-2008 by the American courts [8], electronic contracts have been invalidated in the following cases:

- If it is not possible to prove that the consumer has obviously noted the existence of an electronic contract. (However, if a consumer has noticed the existence of a contract, it will be valid even if the consumer did not read the clauses);
- If the contract has been modified by the powerful party without notifying the weak party ;
- If the electronic contract infringes the traditional doctrines of contract laws (e.g. kids rules, unfairness rules, etc.).

Laws regulating contracts differ between the US and the EU mainly because of the EU directive on unfair contract terms (which regulates contracts offered by merchants to consumers whether online or offline); the distance selling directive (which regulates transactions between remote merchants and consumers, whether by means of television, telemarketing, Internet or other electronic communications medium) and the Electronic Commerce Directive (which promotes transparency and accountability in online commerce) [7]. Annex 1 of the EU directive on unfair contracts contains a list of terms that may be considered abusive. It provides examples of unfair terms. In France, the directive was extended by national legislation to make the use of the French language mandatory. Although countries like Canada, Australia and the UK share a common legal culture with the US, nevertheless their approaches to consumer protection have been similar to the EU approach [9].

In the context of PKIs, a consumer can be at the same time a RP and a certificate holder. CAs try to regularize their relations with RPs and certificate holders through electronic contracts rather than written contracts due to their remote nature. These contracts contain information about different issues, such as: the responsibility and obligations of certificate holders towards the CA and RPs and vice-versa, the identification of the jurisdiction where the dispute will be held in case of problems, the arbitration procedures before filing complaints against a CA, the limitation of a CA's liability, and regulations about holding the personal information of consumers, etc.

Contracts between CAs and certificate holders are generally of type "*clickwrap*", because CAs are always asking the consent of certificate holders when their certificates are issued. Electronic contracts for RPs are of type "*browsewrap*" because these contracts are placed in the extensions of certificates; and a RP must inspect the extensions of a certificate to find the related electronic contract. Given the difficulty of access to the contract, it seems probable that courts would invalidate these contracts because RPs are not usually aware of their existence, and sometimes not even of the certificate. In the EU, if the consumer has not agreed explicitly before the conclusion of a transaction, the contract is not valid. Similarly in the US, courts may consider the contract inadequate when the CA cannot prove the RP has read the conditions of use of a certificate prior to its use. Consequently, different countries try to regulate directly the relationship between the involved parties (CAs, certificate holders and RPs) by issuing explicit laws handling the rights and the liability of each party. This point is presented in detail below.

Differences about the liability of the involved entities. Liability issues play an important role in the relationship between RPs, certificates holders and CAs. Regulating liability issues can be executed in two ways: by contract or by law. Relations between the CA and the certificate holder are contractual, whereas relations between CAs and RPs are not based on contracts in the open model.

Differences between countries about liability issues can be recognized in three main areas: the extent that laws cover the involved parties, the burden of proof and the possibility to limit the liability of CAs. Concerning the extent that laws cover the involved parties, four categories can be identified [5]:

- No specific provisions on liability;
- Provisions on liability rules only for suppliers of PKIs ;
- Rules of liability for certificate holders and suppliers of PKIs;
- Liability rules for all the parties.

The differences between jurisdictions appear also on the designation of the party which has the burden of proof in case of a problem. There are two main options: Ordinary negligence where it is the responsibility of the injured party to demonstrate that the damage was caused by the other party's fault or breach of its obligations, and presumed negligence where a party's fault is presumed whenever damage has resulted from an act attributable to it (e.g. directive 1999/93/EC).

Finally, the ability of the PKI providers to limit their responsibilities has been treated differently between countries. CAs try systematically to limit their responsibilities towards certificate holders and RPs. Although most legal systems recognize the right of CAs to limit or to exclude their responsibilities through contractual arrangements, this right has been subject to various restrictions and conditions [5].

Differences about privacy rules. CAs could have problems related to privacy. To generate certificates, CAs need to collect a set of personal and business information about people requesting certificates. Governments have adopted different approaches to regularize the legal rules related to privacy. The difference between the US and EU approaches to social and economic regulations also influences the rules for the protection of personal information. In the EU, the protection of private information is considered a basic human right. In the US however, the person who collects and stores private information is supposed to be the owner, unless a specific law creates a right for the data subject for a specific type of personal information [10].

3.2 Organizational differences

The organization of a PKI varies from one country to another depending on the level of intervention of governments, which is generally considered in most countries to be a means of trust enhancement. Three main models can be identified [5]:

- *Self-regulation*: In this model, an organization can start up a PKI business without any prior accreditation. No license is required. The US is an example of this;
- *Limited government intervention*: some governments establish a voluntary accreditation system. Under this system, a PKI provider is not forced to search for a license. But licensed PKIs have more advantages than unlicensed PKI providers. The audit of PKIs is normally done by entities accredited by the concerned government. Singapore and the EU are examples of this model;
- *Complete control of governments*: Governments setup mandatory accreditation systems where PKI providers are forced to get a license before starting their business. Governments also conduct the audit process. China and Malaysia follow this model.

The level of technological and administrative maturity in a country plays an important role in determining the appropriate organizational model for PKIs. It is difficult to exclude the intervention of governments in countries whose technological and administrative maturity is not sufficiently developed. In these countries, governments must intervene to facilitate the using of a new technology. Winn et al [11] present an example that shows how the intervention of the Chinese government has contributed to the success of the market in accounting software in China. The study shows that this success was due to government intervention in the market. It shows also that the organizational model of self-regulation for accounting software has been successfully adopted when the market has reached a certain level of maturity.

3.3 Technical differences

It has never been easy to define a common set of standards between countries. The structure of standards developing organizations (SDOs) varies across countries according to their political, economical and legal structures. SDOs in the US operate outside any form of public control and focus solely on market conditions, while the EU SDOs are under government surveillance and are guided by both the social and economic expectations of the market [14].

Winn, J. K. [14, 20] demonstrates this difficulty by contrasting the standardization processes adopted in the US and the EU.

Standardization process in the US. Most standards are developed by private organizations such as the National Fire Protection Association, and the Institute of Electrical and Electronics Engineers (IEEE). In order for a standard produced by these organizations to be recognized as an "American National Standards" by the American National Standards Institute (ANSI), the procedures followed to develop that standard must meet the "essential requirements" established by ANSI. These are designed to ensure fairness in the procedures used for developing these standards [14].

One of the advantages to private organizations of being accredited by ANSI is that it will be easier for them to have their standards submitted to ISO, and they can then get international recognition. However, meeting all the requirements of ANSI could slow the development process, especially since it can be difficult to obtain a consensus from all the participants. For example, some participants who are developing proprietary technologies can deliberately delay the development of a public standard in order to drive the market to adopt their own proprietary technology [14].

The suppliers of IT products need a flexible development process for standards. They prefer generally to work with consortiums because they can adapt more rapidly to market evolutions than the traditional standardization organizations. Consortiums have generally a limited number of participants and simplified development procedures for standards.

In the US, many *de facto* standards exist in the context of PKIs. One of the best known is the "extended validation certificate" standard [15]. It describes a set of technical and legal criteria that CAs must meet in order to generate "extended validation" certificates, which are used to authenticate web servers. The standard is established by a group of commercial CAs and by the producers of well known web browsers such as Firefox and Internet Explorer.

Standardization process in the EU. Governments tend to play a more important role in the elaboration of standards. EU countries usually have one National Standards Body (NSB) responsible for managing all the national standards. The EU has adopted a strategy called the "New Approach" in order to harmonize the efforts of law reform with the efforts of standards' development between the member states. In the New Approach, after the preparation of a directive that defines the "essential requirements" related to one issue, the standardization process will be initiated by one of the three recognized organizations in Europe for the development of standards: the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI). The European Commission (EC) may then send an observer to verify whether the resulting standards meet the essential requirements of the legislation of the directive.

However, it is difficult to adapt the “New Approach” strategy to the development of ICT standards; this is partly because the process of the New Approach to the development of standards is much slower than the simple process of informal standardization followed in the US for developing ICT standards [12].

The EU directive on electronic signatures is a **light version** of the New Approach; unlike the directives based on the traditional New Approach, the electronic signature directive doesn’t require the development of formal standards to support compliance to the directive of electronic signatures [20]. CEN, CENELEC and ETSI have introduced new types of products, such as CEN CWAs (Workshop Agreements), ETSI TS (Technical Specifications) and GS (Group Specifications), for accompanying the rapid evolution of the ICT market, and for facing the growing influence of international consortia working outside the EU. These products provide an alternative to the formal rigid process of standardization for the development of formal European Norms (ENs).

The work of developing standards for electronic signatures has been entrusted to the “European Electronic Signature Standardization Initiative” (EESSI). EESSI is an ad hoc body set up under the aegis of “the Information and Communications Technologies Standards Board (ICTSB)”, an organization that specializes in coordination between the European standards bodies CEN, CENELEC and ETSI. EESSI’s work was completed in 2003 and published in the Official Journal. As a consequence, the differences in strategies for developing standards have resulted in different standards in the domain of PKIs.

3.4 Discussion

Neither the US nor the EU has found an effective way to promote the adoption of PKI technologies. In the US, the removal of legal, technical and organizational barriers in the market of PKIs has not led to the establishment of strong mechanisms for authentication and signatures. By promoting the unregulated competition among providers of identity technologies, many technical solutions have been deployed in the market, but none of these solutions has really dominated the market. Consequently, identification and authentication for Internet transactions in the US remain mainly based on UserID/Password; despite the well known security problems associated with them [12]. In February 2005, the Federal Deposit Insurance Corporation released a report indicating the severity of the problem of identity theft in the US and concluded that reinforcing online identification systems is essential to solve the problem. This is why the Obama administration is trying to reduce fraud on the Internet by developing an ecosystem for online identity management at the national level. The administration is currently working on the National Strategy for Trusted Identities in Cyberspace. A draft of the proposal was publicly released at the end of June 2010 [13]. The identity ecosystem is based on four main principles:

- The system will be secure and resilient;
- The system will be interoperable;
- The system will be privacy-enhancing and voluntary;
- The system will be cost-effective and easy to use.

However today, in the context of PKIs, the situation in the US remains unclear. Users must be able to assess the technical and legal risk resulting from the dependence on various PKIs, which utilise different types of certificates with different levels of technical and juridical qualities.

In other countries, such as the EU, which provide a minimum level of technical and legal protection for their citizens, the clarity of the situation at national level increases with the government's level of intervention. However, the international situation remains unclear. These countries have problems regarding the recognition of foreign certificates managed by foreign PKIs. For example, web browsers imposed the "extended validation" standard as a *de facto* solution for recognizing these certificates. Given the approach that has been followed for developing this standard, the EU countries could find this standard unfair to their citizens. Currently, there are not sufficiently well developed mechanisms to give official recognition to the standards developed outside the EU's borders.

The various attempts that have been aimed at harmonizing the trust frameworks of PKIs between countries have not actually improved the situation. For example, the attempt by the United Nations Commission on International Trade Law (UNCITRAL) to harmonize the laws of different countries for the recognition of electronic signatures has not achieved its objectives. The proposed harmonizing approach is flexible; it allows countries that have adopted it to modify it freely to suit their own needs. But this has led to creating interoperability problems [17].

In the EU, the legal, technical and organizational harmonization through the directive on electronic signatures has not been a huge success. In 2007, a study, at the request of the EC found that the lack of interoperability between EU countries is one of the main factors that have contributed to the slow adoption of electronic signature technology in Europe [18]. In fact, in parallel with the standardization efforts of EESSI, some Member States have developed their own national standards such as ISIS-MTT in Germany, PRIS in France and SEIDE in Sweden. These standards have created additional interoperability problems between European countries. This is legally possible in the EU because CWAs and TSs don't have the same status as formal standards (ENs). Therefore, the obligation imposed on Member States to remove existing national standards that are inconsistent with European standards does not apply in the case of CWAs and TSs [19].

To face this problem, the EC is working on a new proposal to regulate electronic identification and trust services for electronic transactions in the internal market [23]. The objective of this proposal is to enable cross-border secure transactions between European countries, both for the public and private sectors. Whilst directive 1999/93/EC only covers electronic signatures, the new regulation defines a comprehensive framework that encompasses electronic identification, authentication and signatures. It is too early to measure the success of the new regulation. However, the new regulation introduces certainty only for qualified trust services i.e. those that meet the requirements of the EC, and not other trust services that nevertheless are still authorized to sell their services in the EU market. Thus, uncertainty will still persist for the latter services.

Today, new countries are starting to have an important role in the development of global standards (especially China, India and Korea). For example, Scott Kennedy explains [16] that the investment of China in standards development is to break the domination of western countries in this area. The quality of these standards can vary considerably, depending on the participants and the rules for participation established by the agency that develops the standards.

As a consequence of these major differences, PKIs remain isolated islands in the open model. Each PKI seeks to comply only with the requirements of the jurisdiction where the premises of its root CA are located. Thus, the RPs have to handle this PKI interoperability issue in the end. The various harmonization attempts at regional and international level have not come up with a solution to the PKI interoperability problem. Trust architectures such as Bridge CAs or hierarchical CAs cannot help in resolving the problem in the open model since the main idea of these architectures is to prove the juridical, political and technical equivalence between CAs. However, because of the interoperability problems between countries, this equivalence is not feasible. This is why Web browsers today contain many hierarchical CA roots, and not just one.

4 Handling the interoperability problem from the trust management point of view

The persistence of interoperability problems creates a ***trust management problem***, i.e. how can an RP trust one CA or another when certificates have different levels of quality? If there was a compatibility between PKIs at the juridical, organizational and technical levels, there would not exist a ***trust management*** issue because in this case a limited number of classes of globally accepted certificates could be defined, where each class could meet a specific context of use. However, this theoretical solution cannot be implemented in practice because of the reasons presented in section 3.

We propose to handle the interoperability problem by transforming it into a ***trust management problem***. Establishing trust in a certificate requires managing technical, organizational and legal issues. This task is extremely complex, therefore only technical and legal experts can perform it. It is not conceivable to delegate this task to the RPs which generally are unskilled people.

In the closed PKI model, the administrators of the CAs and the lawyers of each organization play the roles of technical and legal experts to help the employees of the organization in dealing with certificates coming from other organizations. RPs and the experts, being part of the same organization/company, have a trust relationship which is naturally created. The trust of the RPs in their administrators is not only related to the quality of the certificates they are issued with but also to the CAs they are recommended or allowed to trust. In addition, interconnection topologies are often built for a predefined number of services related to the nature of the collaboration between the organizations. Thus, the trust decisions of the RPs can be automatically configured.

In the open model, the situation is far more complex than the closed model for several reasons (**Fig. 3**). There is no explicit and balanced predefined trust relationship between RPs and experts. Web browsers implicitly play the role of expert as they manage the list of trusted CAs, but there is no agreement between the RPs and the browsers' manufacturers to make them responsible for the information they provide.

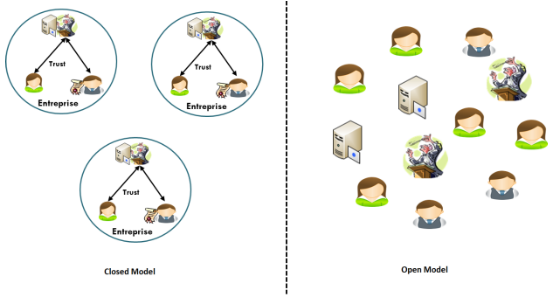

Fig. 3. Differences between the closed model and the open model

Secondly, the scope of the certificate usage is more open (i.e., not limited to predefined specific services). The consequence is that Web browsers don't provide enough information to make an informed decision. The recommendation is binary (trusted or not recognized, e.g. an icon in the URL bar is blue or not). Trusted CAs are all stored in the same trusted list. CAs with different levels of quality are equally trusted regardless of the use of the certificate.

All these **ad-hoc** solutions, either for the open (e.g. Web browser approach) or for the closed model (e.g. interconnection topologies), include **implicitly** the role of expert. The differences lie in the nature of the entities playing the role of expert, the type of trust linking the expert with the RPs, and the nature of the information that the expert supplies to RPs. We propose to clarify this situation by adding **explicitly** the role of a trusted expert to the X.509 trust model, in the form of a **trust broker**. RPs need to rely only on the trust broker and not on each and every CA issuing certificates to their holders. In this case, the X.509 trust model is fairer for the RPs. The trust broker evaluates objectively the CA and its certificates, and sends recommendations to RPs that helps them to make informed decisions about these certificates (**Fig. 4-A**).

The relation between the trust broker and the RPs must be regularized by **explicit** agreements. In such agreements, the trust broker recognizes its **responsibility** to the RPs about the provided recommendations and requires itself to respect and to protect the privacy of the RPs. On the other side, the trust broker must be **independent** from the CAs. Its relationship with CAs must also be regularized by **explicit** agreements, so that the trust broker can transfer the responsibility to a CA when a false recommendation is made resulting from incorrect information provided by the CA.

The contractual agreements between the RPs and the trust brokers create trust communities. The role of trust broker could be provided by:

- Commercial organizations which make a business from giving recommendation about certificates;
- National governments which wish to facilitate e-commerce in their countries;
- An international body like the UN in order to facilitate international trade.

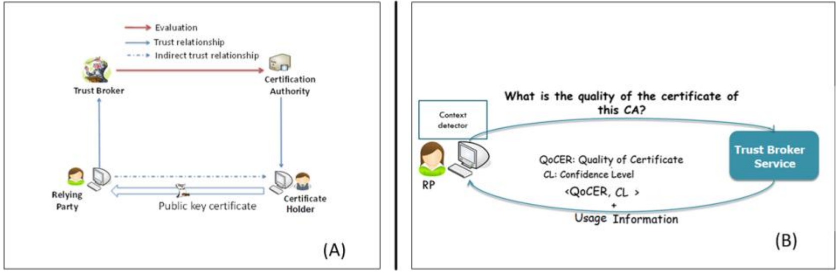

Fig. 4. The Trust Broker

Finally, to help RPs to make informed decisions about certificates, the trust broker must provide **contextual recommendations**. For example, recommendations about a certificate that authenticates an email server should be different from recommendations about a certificate that authenticates an e-commerce server. This is because the information sent by the RP to the certificate holder (login/passwd or credit card information) and the consequences of these transactions are different. In the first case, the critical information is the quality level of the certificate and the financial and juridical protection if the certificate is false. In the second case, this information should be supplemented with the maximum transaction amount that can be used in order to stay covered by the financial protection offered in the CP/CPS.

We have already proposed that the next version of X.509 contains the trust broker as a new trusted third party for RPs, and the current working draft of X.509 (2016) [24] contains the four cornered model shown in **Fig 4-A**. We have also started an implementation of a trust broker service and protocol. We call it the "unified approach" because it is applicable to both the open and closed deployment models of PKIs (**Fig. 4-B**). When an RP receives a certificate, its client sends a query to the trust broker asking it about the trustworthiness of the certificate. The trust broker responds by providing three types of information:

- Quality of Certificate (QoCER): a score between 0 and 1 representing the level of trust that can be placed in the certificate;
- Confidence Level (CL): a score between 0 and 1 that indicates to what extent the trust broker is confident in the QoCER recommendation sent to the RP;
- Usage information about the recommended or allowed uses of the certificate.

The RP's proposed certificate's use is only provided to its client rather than to the trust broker for privacy reasons. Consequently the trust broker has to enumerate all the allowed uses for the certificate. This list should be structured enough to allow the client to match the appropriate use and present this to the RP. For example, the list could contain: {"Bank Server authentication", "E-mail server authentication", "Buying a product with 5000$ maximum", "multimedia server authentication", etc.}. Part of our future research is to determine the way this information should be structured in order to allow efficient matching. If there is no intersection between the proposed use and the trust broker's list, then the client will recommend the RP not to use the certificate. Further information about the calculation of OCER, CL and the usage parameters can be found in [22]. Once we have finished the pilot implementation we propose to offer the protocol to a standards body such as the IETF of OASIS.

A direct application of our work could be to help RPs to decide about the juridical validity of a digital signature apposed on a document. The juridical validity of a digital signature depends in part on the quality of the CA's management procedures of the certificate used to validate the signature. The score of QoCER represents in this case the juridical validity of the signature and can help the RP to decide whether to accept the signed document or not.

In previous research, Jon Olnes [21] introduced a new entity, called a "Validation Authority" (VA), to help RPs take decisions about certificates. It is similar to our concept of a trust broker. The relationship between a VA and RPs must be regularized through contractual agreements. However, the interoperability differences between countries are not explained and thereby the role of the VA is not completely justified. Additionally, the author doesn't provide information about the nature of recommendations to send to RPs. Finally, the concept of contextual recommendations is not considered.

5 Conclusion

X.509 certificates have been widely adopted today for the realization of different security services. However, many problems still slow the adoption of this technology by (mainly human) RPs, one of them being the interoperability problem. One of the objectives of this paper was to clarify the interoperability problem and we have shown that juridical, organizational and technical differences between countries are the main reasons for this problem. We have proposed to solve this from a trust management perspective, by extending the X.509 trust model to include a new trusted third party called the trust broker. We have also started to implement this role as a new TTP service to be offered to RPs.

References

1. Hanna, S. R., Pawluk, J.: Identifying and Overcoming Obstacles to PKI Deployment and Usage. In: 3rd Annual PKI R\&D Workshop. NIST, Gaithersburg MD (2004)
2. Smith, P.: Internet Based Payments Application - Trust and Digital Certificates. In: 16th Payment Systems Internatoinal Conference (PSIC). Bruges, Belgium (May 2000)
3. Organization for Economic Co-operation and Development (OECD): The OECD report on regulatory reform: Synthesis, http://www.oecd.org/dataoecd/17/25/2391768.pdf. Paris (1997)
4. PKI Assessment Guidelines of the American Bar Association, http://www.abanet.org/scitech/ec/isc/pagv30.pdf

5. United Nations Commission on International Trade Law: Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods. ISBN 978-92-1-133663-4 (2009)
6. Susanna, F. Fischer: Saving Rosencrantz and Guildenstern in a virtual world? A comparative look at recent global electronic signature legislation. In: Journal of Science and Technology Law, vol. 7. (2001)
7. Deffains, B., Winn, J.K.: Governance of Electronic Commerce in Consumer and Business Markets. In: Social Science Research Network, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1099516 (2008)
8. Moringiello,J. M., Reynolds, W. L.: Survey of the law of CyperSpace Electronic Contracting Cases 2007-2008. In: Business Lawyer 64 (2008).
9. Winn, J. K., Bix B. H.: Diverging Perspectives on Electronic Contracting in the US and EU. In: Clev. St. L. Rev. 54: 175 (2006)
10. Winn, J. K.: What protection do consumers require in the information economy?. In: Law Ethics & Society 4: 84–102 (2008)
11. Winn, J. K., Yuping, S.: Can China Promote Electronic Commerce through Law Reform-Some Preliminary Case Study Evidence. In: Colum. J. Asian L. 20: 415 (2006)
12. Winn, J. K., Jondet, N.: A ‘New Approach’ to standards and consumer protection. In: Journal of Consumer Policy 31 (4): 459–472 (2008)
13. National Strategy for Trusted Identities in Cyberspace, Daft (2010)
14. Winn, J.K.: Information Technology Standards as a Form of Consumer Protection Law. Available at: http://www.law.washington.edu/Directory/docs/Winn/Info_Tech_Stds.pdf. (2008)
15. Guidelines for the issuance and management of extended validation certificates. Available at: http://www.cabforum.org/EV_Certificate_Guidelines.pdf. (2007)
16. Kennedy, S.: The political economy of standards coalitions: Explaining China’s involvement in high-tech standards wars. In: asia policy 2: 41–62 (2006)
17. Martínez-Nadal Apollònia, Josep Ferrer-Gomila: Comments to the UNCITRAL Model Law on Electronic Signatures. In: Information Security, 229-243. (2002)
18. European Commission: The study on the standardisation aspects of eSignatures. http://ec.europa.eu/information_society/eeurope/i2010/docs/esignatures/e_signatures_standardisation.pdf. (2007)
19. Van Eecke, P., Pinto Fonseca, P., Egyedi, T.: EU Study on the specific policy needs for ICT standardisation: Final report. (2007)
20. Winn, J. K.: US and EU regulatory competition and authentication standards in electronic commerce. Journal of IT Standards and Standardization Research, 5(1), 84–102. (2006)
21. Ølnes J.: PKI Interoperability by an Independent, Trusted Validation Authority. In: 5th Annual PKI R&D Workshop 2006 (2006).
22. Wazan, A.S., Laborde, R., Barrère, F., Benzekri, A.: A formal model of trust for calculating the quality of X.509 certificate. In: Security and Communication Networks 4(6): 651-665 (2011).
23. Draft Regulation on “electronic identification and trusted services for electronic transactions in the internal market” (2012).
24. ITU-T Rapporteur Q.11/17. “Rec. ITU-T X.509 (2012) | ISO/IEC 9594-8 : 2012 Information Technology - Open systems Interconnection - The Directory: Public-key and attribute certificate frameworks – Working Draft for Adm. 2: Directory-IdM support.” TD0241, Geneva, 17-26 April 2013