Proposition summary to X.509 committee: Adding the Role of technical and juridical expert to X.509 trust model

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

[1]Telecom Sudparis, SAMOVAR UMR 5157, 91011 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

1 Problem summary

The X.509 trust model includes three entities: the certification authority (CA), the certificate holder and the relying party (RP). In this model, the certificate holder depends on the CA for the provision of his certificate and the RP depends on the CA for the validity of the certificate's information (Figure 1).

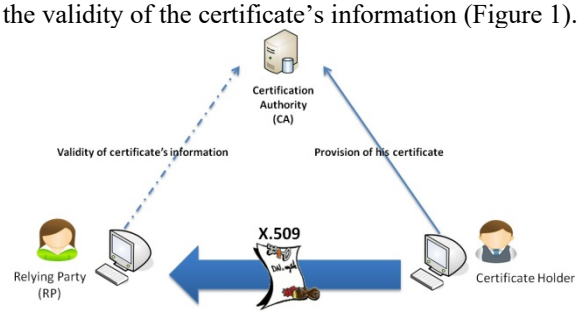

Figure 1. The current X.509 trust model

The X.509 trust model is only appropriate for the closed deployment model of PKI, in which the RPs and the subjects both have relationships the CAs. It is not appropriate for the open deployment model where the RP has no explicit relationship with the CA. 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. Cross-certified CAs, bridge CAs are example of the closed model. However, in the open model, which applies to the Internet today, there is no explicit contractual relationship between the CA and the relying parties (RPs).

As a consequence, RPs have to build their trust decision by analyzing a set of CA documents (CPs, CPSs) to answer many technical and legal questions like: What happens when a CA does not correctly check the identity of the certificate holder, or worse, when it issues a certificate to a person with a false identity? What happens if the certificate is false and makes me lose 1000€? Is the CA responsible? Etc.

The main complexity of the open model comes from these PKI interoperability issue. In fact, PKIs have been regulated through two different mechanisms: economic regulations and the social regulations. The objective of economic regulation is to increase the economic efficiency of PKIs by reducing barriers to competition and innovation, often by deregulation. The objective of social regulation is to protect public interests such as health, safety and the environment. Thus, the main goal being social welfare, the economic interests of social regulations are a secondary concern.

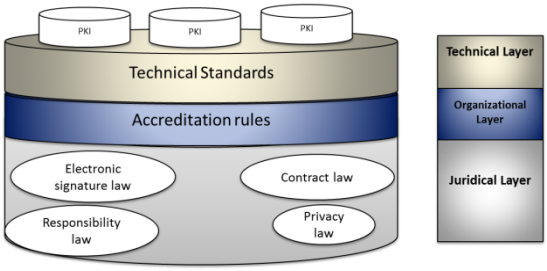

Figure 2. PKI regulation layers

Regulating PKIs should be performed at three different levels: juridical, organizational and technical (Figure 2). At the juridical level, the implementation of PKIs requires the processing of different legal issues: juridical validity of electronic signatures, juridical validity of electronic contracts, legal responsibilities of CAs, certificate holders and RPs, and privacy rules. All these issues have been treated differently between countries. Generally, the legal differences that exist today come from the unequal legal traditions (civil law and common law) followed in the different countries.

At the organizational level, three main approaches can be identified:

- *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 apply 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 by 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.

At the technical level, it is not easy to define a common set of standards between countries. The structure of standards developing organizations (SDO) varies across countries according to their political, economic and legal structures. SDOs in the U.S. operate outside of any form of public control and focus solely on market conditions, while the European SDOs are under government surveillance and are guided by both social concerns and the expectations of the market. Thus, this situation has resulted in different technical standards in the domain of PKIs. In the US, many *de facto* standards exist in the context of PKIs. One of the best known is the "extended validation" standard. 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.

Thus, there is no 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 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.

Consequently the situation of PKIs in the US remains unclear. Users must be able to assess the technical and legal risk resulting from the dependence on various PKIs, which utilize 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.

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. 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.

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.

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

CAs are supposed to help RPs establishing trust in certificate holders. But this is not the case in the open model, because RPs need first to trust CAs. In fact, 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 differences in regulation strategies followed by different countries.

We can 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 PKI 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 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 (**Figure 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.

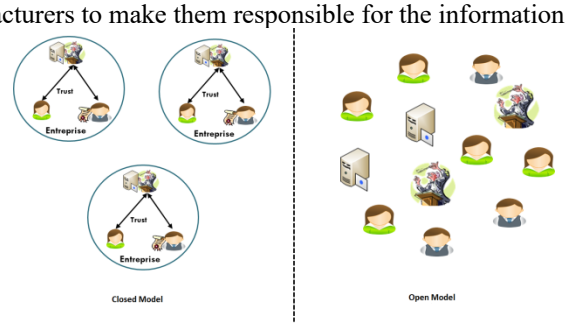

Figure 3. Differences between the closed model and the open model

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 a full 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 trust 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 **expert trusted third party** to the X.509 trust model. RPs need to rely only on the expert 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.

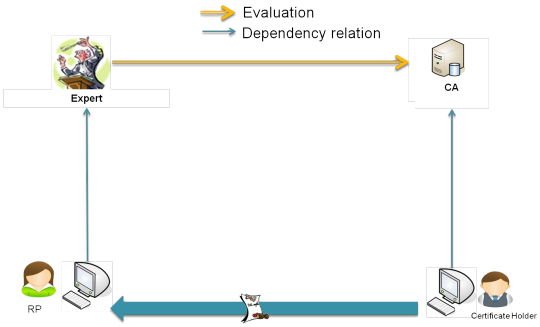

Figure 4. The proposed X.509 trust model

The expert evaluates objectively the CA and its certificates, and sends recommendations to RPs that helps them to make full informed decisions about these certificates (**Figure 5-A**). The relation between the expert and the RPs must be regularized by **explicit** agreements. In such agreements, the expert 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 expert must be **independent** from the CAs. Its relationship with CAs must also be regularized by **explicit** agreements, so that the expert 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 experts create trust communities. The role of expert trusted third party 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.

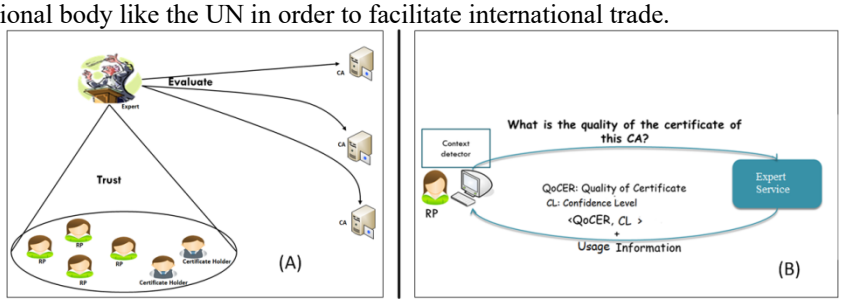

Figure 5. The technical and juridical expert service

Finally, to help RPs to make full informed decisions about certificates, the expert 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 started an implementation of an expert TTP service for managing the trust in X.509 certificates. We call it the "unified approach" because it is applicable to both the open and closed deployment models of PKIs (**Figure 5-B**). When an RP receives a certificate, its client sends a query to the expert service asking about the trustworthiness of the certificate. The expert service 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 service 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 expert for privacy reasons. Consequently the expert 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 expert's list, then the client will recommend the RP not to use the certificate.

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.

3 Conclusion

X.509 certificates have been largely adopted today for the realization of different security services. However, the X.509 trust model does not consider the problem of trust management in open systems when multiple and isolated CAs exist. The objective of this summary is to show the necessity of extending the X.509 trust model to include the role of technical and juridical expert. All the **ad-hoc** solutions applied today, either for the open or for the closed model of PKIs, include **implicitly** this role of expert. We are proposing to clarify this situation by adding **explicitly** in the X.509 trust model this new role. In this case, the new trust model would include four entities: CA along with certificate holders and experts along with RPs. The certificate holders are protected by their CAs and RPs are protected by the experts through contractual relations.

4 References

1. A.S. Wazan, R. Laborde, F. Barrère and A. Benzekri, A formal model of trust for calculating the quality of x.509 certificate, *Security and Communication Networks* 4(6) (2011), 651–665.
2. A. S. Wazan, R. Laborde, F. Barrère and A. Benzekri, "The X.509 trust model needs a technical and legal expert," 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, 2012, pp. 6895-6900, doi: 10.1109/ICC.2012.6364860.
3. A. S. Wazan, R. Laborde, F. Barrère and A. Benzekri, "Validating X.509 Certificates Based on their Quality," 2008 The 9th International Conference for Young Computer Scientists, Hunan, 2008, pp. 2055-2060, doi: 10.1109/ICYCS.2008.75.
4. A.S. Wazan, R. Laborde, F. Barrere, A. Benzekri., D.W. Chadwick « PKI Interoperability: Still an Issue? A Solution in the X.509 Realm ». In: Dodge R.C., Futcher L. (eds) Information Assurance and Security Education and Training. (2013) WISE 2013. IFIP Advances in Information and Communication Technology, vol 406. Springer, Berlin, Heidelberg