How Can I Trust an X.509 Certificate? an Analysis of the Existing Trust Approaches

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

To cite this version:

Ahmad Samer Wazan, Romain Laborde, David W. Chadwick, François Barrère, Abdelmalek Benzekri. How Can I Trust an X.509 Certificate? an Analysis of the Existing Trust Approaches. 41st IEEE Conference on Local Computer Networks (LCN 2016), Nov 2016, Dubai, United Arab Emirates. pp. 531-534. hal-01690136

HAL Id: hal-01690136
https://hal.science/hal-01690136v1

Submitted on 22 Jan 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Open Archive TOULOUSE Archive Ouverte (OATAO)

OATAO is an open access repository that collects the work of Toulouse researchers and makes it freely available over the web where possible.

This is an author-deposited version published in : http://oatao.univ-toulouse.fr/
Eprints ID : 18789

The contribution was presented at LCN 2016 :
https://www.ieeelcn.org/prior/LCN41/

To cite this version : Wazan, Ahmad Samer and Laborde, Romain and Chadwick, David W. and Barrère, François and Benzekri, Abdelmalek *How Can I Trust an X.509 Certificate? an Analysis of the Existing Trust Approaches.* (2016) In: 41st IEEE Conference on Local Computer Networks (LCN 2016), 7 November 2016 - 11 November 2016 (Dubai, United Arab Emirates).

Any correspondence concerning this service should be sent to the repository administrator: staff-oatao@listes-diff.inp-toulouse.fr

How Can I Trust an X.509 Certificate? An Analysis of the Existing Trust Approaches

A.S. Wazan[1], R. Laborde[1], D.W. Chadwick[2], F. Barrere[1], And A. Benzekri[1]
[1] *IRIT Laboratory, Paul Sabatier University*
{ahmad-samer.wazan, laborde, barrere, benzekri}@irit.fr
[2]*University of Kent*
d.w.chadwick@kent.ac.uk

Abstract— A Public Key Infrastructure (PKI) is based on a trust model defined by the original X.509 standard and is composed of three entities: the Certification Authority, the certificate holder (subject) and the Relying Party. The CA plays the role of a trusted third party between the subject and the RP. A trust evaluation problem is raised when an RP receives a certificate from an unknown subject that is signed by an unknown CA. Different approaches have been proposed to handle this trust problem. We argue that these approaches work only in the closed deployment model where RPs are also subjects, but cannot work in the open deployment model where they are not. Our objective is to identify the deficiencies in the existing trust approaches that try to help RPs to make trust decisions about certificates in the Internet, and to introduce the new X.509 approach based on a trust broker.

Index Terms— Public Key Infrastructure, X.509, Certification Authority, Trust management, Trust Broker.

I. Introduction

A Public Key Infrastructure (PKI) is based on the trust model described in the original X.509 (1988) standard and is composed of three entities: the Certification Authority (CA), the certificate holder (or subject) and the Relying Party (RP). The CA plays the role of a trusted third party (TTP) between the subject and the RP. This trust model is only appropriate for the closed deployment model of a PKI, in which the RPs and subjects are all certificate holders with the same set of CAs. It is not appropriate for the open deployment model where the RP has no explicit relationship with any CA. This is because RPs are now supposed to build their trust decisions by analysing a set of CA documents (Certificate Policy (CP) and Certification Practice Statement (CPS)) to answer many technical and legal questions like: what happens when the CA does not correctly check the identity of the certificate holder, or worse, issues a certificate to a person with a false identity? What happens if the certificate is false and I lose $1000? Is the CA responsible? etc. [2]. This is an impossible task for most RPs.

We believe that helping RPs in the open model to make informed decisions about a certificate's trustworthiness entails the following steps:

1. Defining a new model of trust: In previous work [7], we proposed to add a new role of Trust Broker (TB) to the X.509 model, which contracts with RPs to help them make an informed decision about a CA (i.e. whether to accept a subject's certificate for a particular transaction or not). This new entity should be independent of PKIs and play the roles of both technical and legal expert for the RPs. By explicitly adding this trusted role to the original X.509 trust model, the task of RPs is simplified, and the responsibility of the TB can be formally engaged. This new four cornered trust model (see Fig. 1) is now incorporated into the ITU-T draft amendment to the 2016 edition of X.509,
2. Specifying protocols for the interaction of TBs with CAs and RPs,
3. Building software tools to help RPs and TBs participate in this new trust eco-system.

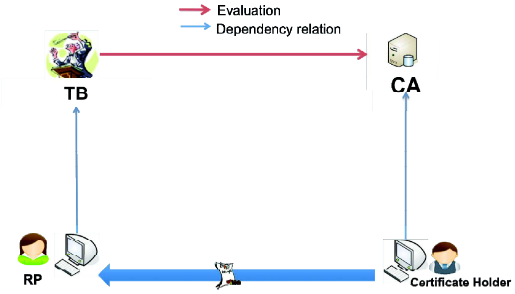

Fig. 1.The new X.509 trust model

The main objectives of this paper are to identify the deficiencies in the existing trust approaches for helping RPs to make informed decisions about certificates, and to provide a brief outline of steps 2. We demonstrate that none of existing trust approaches help RPs when they encounter unknown certificates in the open model.

The analysis of the deficiencies led us to define a new trust management approach, called the Unified Approach. It combines the advantages of the existing trust approaches, and is applicable to both the closed and the open PKI deployment models. We terminate this paper by concluding our analysis and presenting our future work.

II. Analysis of the Existing Trust Approaches

There are several alternative approaches that permit a RP to trust a certificate. These approaches entail two important mechanisms:

- A contractual process for recognizing CAs: this is used to prove that a given CA meets the legal and technical requirements of trustworthiness and interoperability.

- A mechanism for conveying the recognition of trustworthy CAs into the RPs computer system: this is used to provide information about the trustworthiness of a CA in a machine-readable format, so that when the RP receives a digital certificate it can automatically decide to accept it or not. This is achieved via configuration of at least one root of trust, or trust anchor, into the RP's system by some out of band means. Subsequently certificate chains can be carried in an application level protocol. Providing the chain starts at an already configured root of trust, then the entire set of CAs in the certificate chain can be trusted. If it does not, then the entire set of CAs will be untrusted. There are several topologies to facilitate the building of certificate chains: the hierarchical topology, web of trust topology and the bridge topology.

The existing approaches can be classified into two main categories: (1) trust topologies managed by CAs themselves and (2) a list of roots of trust managed by the RP or by a trusted third party (TTP) that is independent of the CAs and is acting on behalf of the RP. The aim of this section is to present these approaches. In each approach, we discuss the transmission mechanisms, the political process and the applicability of the approach to the open and closed deployment models.

A. Inter-CA Trust Topologies

CAs can build trust topologies between themselves instead of leaving this task to inexperienced RPs. The main idea is that each RP trusts a CA (called a root of trust or trust anchor), which in turn certifies other CAs for its RPs. Thus, in these topologies, CAs play two roles: Certificate Manager and certificates recommender. Trust relationships between CAs are technically formalized using cross-certificates issued to each other.

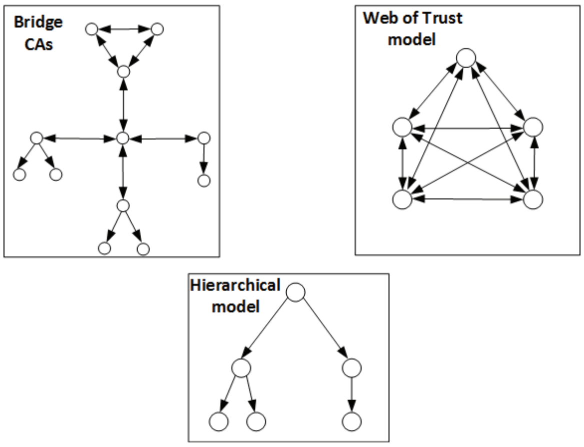

Fig. 2.Trust Chain Topologies

The trust chains can be organized in a hierarchy, web of trust or via a bridge CA as illustrated in Fig. 2. Each arrow depicts the direction of a trust link. In CA hierarchies, the trust chains flow from the superior CA to the subordinate CAs, whereas in a Bridge CA topology the trust chains flow in both directions through the Bridge. In a web of trust, the trust chains are ad-hoc and random. These topologies are used to transmit the recognition of a certificate to the members of the interconnected domains. In these topologies, a certification path must be established between the RP and the certificate holder in order to check the validity of a certificate. The certification path starts from a trust anchor of the RP and ends with the subject's certificate.

All these topologies are based on one process called cross certification. Currently, there is no standardized process for cross-certification, which covers legal, political and technical assessments. One of the most detailed processes is that defined by the Federal Public Key infrastructure (FPKI) [6]. It gives explicit documentation about each step, as follows:

- Presentation of the request: The applicant CA must provide a formal written request to the FPKI Policy Authority (FPKIPA) containing certain information.
- Policy mapping process: the criterion-by-criterion comparison of the certification policy of the applicant CA with the CP of any one of the CAs of the FPKI to assess whether the policies, practices and procedures of the applicant have an equivalent level to those of the CAs of the FPKI.
- Audit examination: The applicant CA must provide assurance that its operations reflect perfectly its CP and CPS. It must undergo a compliance audit by a qualified independent auditor who meets the criteria requested by the FPKI.
- Technical test of interoperability: The applicant CA must be technically compatible with the FPKI. The technical compatibility is determined by the examination of the technical information provided by the applicant CA.
- Negotiation for the establishment of an agreement: in order to conclude a common consensus of all points.
- Maintenance: provides mechanisms for managing the cross-certification relationships between the different entities and to terminate an agreement if one party does not fulfil the terms and conditions of the cross-certification agreement.

Inter-CA topologies are usually applied to the closed deployment model of PKIs. However, the implementation of inter-CA topologies in the open model, where all the CAs in the world are interconnected, is not feasible. One could imagine a topology composed of cross certified national root CAs in which each root CA manages cross certification processes with their subordinate CAs located in their jurisdictions. However, even this cannot be easily achieved for several reasons:

1. Technically, this topology cannot be implemented because of the difficulty of managing long certification paths [5]. The validation process requires several checks to be made along the certification path (e.g. policy constraints, certificate status, policy mappings, etc.). The complexity increases with the size of the certificate chain.
2. This topology is similar to a general accreditation system where all CAs must be certified by their national authorities. However, countries do not have the same

viewpoint concerning the right organizational model of PKIs. For certain countries, national accreditation may limit innovation and competition between CAs.

3. Imagining that the national CAs (root or bridge) can cross certify each other implies that a technical and legal harmonization can be conceived between different nations. In reality this is too difficult to achieve because of cultural and legal differences between countries.
4. This topology requires a standardization of the certification process so that a cross-certification realized by one national CA would be accepted by other national CAs. However, there is no standard cross certification process today.

B. Recognition by an RP or an Independent TTP

Trust in a certificate can be recommended by any entity independent of CAs. The basic idea is that users in a given community of interest can obtain information and advice from the leader of this community about the relevance of certificates for their electronic transactions. The recommender should have a technical and legal expertise sufficient to inform its users about the relevance of a certificate for a given type of transaction. The recommender could be a government (e.g. PKI Gate-Keeper in Australia [1]), or any organization such as a software vendor (e.g. Microsoft or Mozilla).

In general, the recommenders create a list of minimum requirements and recognize all CAs whose certificates have assurance levels greater than the minimum requirements. Web browsers are the best-known examples of this approach (Microsoft Root Certificate Program [3], and Mozilla CA Certificate Policy Inclusion [4]).

In contrast with the previous approach, this approach has only one mechanism used to transmit the recognition of certificates, which is the trust list. There is no homogeneous way to define or formalize the trust lists. While some lists of certificates are just simple lists (e.g. stores of certificates in Web browsers) where RPs can themselves add, edit, or delete certificates; others can be signed lists by the recommender where RPs cannot modify the list. From an interoperability viewpoint, the trust list replaces the cross-certificates used in inter-CA topologies. The user trusts the issuer of the list and transitive trust extends this to the CAs contained in the list. As a consequence, the issuer of the list plays the role of trust anchor, but is not a CA.

The trust list topology may be built using a political process called the cross recognition process. This process is defined by the Telecommunications Working Group of the Asia Pacific Economic Cooperation (APEC) forum as "*An interoperability arrangement in which a relying party in one PKI domain can use authority information in another PKI domain to authenticate a subject in the other PKI domain, and vice versa*" [8].

Cross-recognition differs from cross-certification by the fact that it is not performed by a CA. Another difference is that cross-recognition requires only political and legal arrangements and leaves the technical compatibility issues to applications. Finally, cross-recognition requires no mechanisms for handling certification paths.

Currently, there is no standardized process for cross-recognition. The recognition process of the Australian PKI Gatekeeper [1] is considered one of the most documented processes. It provides a rigorous accreditation process for organizations and service providers that wish to issue digital certificates to be used by government agencies. It also provides a mechanism for interoperability based on cross-recognition to help Australian Government departments (i.e. RPs) make decisions about external certificates from PKIs that are not accredited by the Gatekeeper.

The Gatekeeper process of cross-recognition requires a harmonization of policies between the two PKI domains. Before accepting the cross-recognition of a particular domain, the competent authority in the Gatekeeper PKI must ensure that the authorities in the non-Gatekeeper impose requirements and standards that are comparable to those of Gatekeeper PKIs. Another assurance mechanism is the commitment of the recognized PKI to undergo regular audits. The Gatekeeper cross recognition process includes the following steps:

1) Information sharing => 2) Gap analysis => 3) Risk evaluation => 4) Risk attenuation => 5) Negotiation => 6) Policies harmonization => 7) Documentation => 8) Signing agreements => 9) Maintenance and surveillance.

Both authorities in the concerned PKIs start by exchanging detailed information about their PKIs, and then apply a gap analysis to identify the differences between them. They conduct a risk evaluation process to determine whether these differences are significant or not. If they are important, the cross-recognition is not granted by the Gatekeeper authority. The harmonization of policies between the two domains requires several inspections, in particular:

1) The status of the standards applied in every domain whether they are international or not, 2) The legal status of certificates in each domain, 3) Data privacy laws, 4) Liability regimes, 5) Consumer protection laws, and 6) Audit requirements.

Several steps of this process are similar to those of the cross-certification process that was presented in the previous section; the only major difference is the absence of steps to achieve compatibility of the techniques such as configuration directories and certificate profiles.

Thanks to the independence of the recommender from CAs and the absence of need to build certification paths for the validation of certificates, the recognition approach is more convenient to the open deployment model of PKIs. However, the current application of this approach is not optimal for the open deployment model, for several reasons:

1. The nature of the RP's relation with the recommender is not formally defined. It can be formal as in the case of the Gatekeeper strategy or non-formal as in the case of web browsers,
2. The cross-recognition process is a manual not-reproducible

process; it is performed manually by experts who should examine very large documents that include a lot of political and legal information,

3. This approach provides only a binary response, recognized or not. Unrecognized certificates are not banned to RPs since they are constantly exposed to them and a decision must be made. For unrecognized certificates, RPs may still be invited to inspect the policies of CAs to decide whether the certificates are suitable for their transactions or not. The best known example is the web browser, when RPs receive certificates signed by CAs that are not included in the trust list of their browser. The RP is asked to take a decision about the untrusted CA's certificate.

III. The Unified Approach: A New Trust Approach for Helping RPs

We use the term "Unified Approach" to indicate the applicability of our approach to both the open and closed deployment models of PKIs. Our approach combines the advantages of the current trust topologies. It can help RPs to make the correct decisions about certificates.

We propose a set of quantitative and qualitative information that explains the quality of a CA's certification process to RPs. The Trust Broker (TB), as proposed in the new X.509 trust model, can setup a service that provides this information to RPs (Fig. 3) on demand. The retrieval of recommendations can therefore be made simple and dynamic. Furthermore, there is no need to handle long certificate validation paths as is the case for inter-CA topologies.

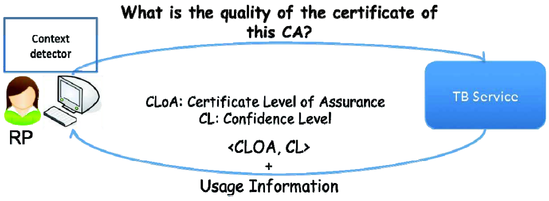
What is the quality of the certificate of this CA?
Context detector
RP
CLoA: Certificate Level of Assurance
CL: Confidence Level
<CLOA, CL>
+
Usage Information
TB Service

Fig. 3. The TB Service and Protocol

At the quantitative/qualitative level, we propose that the TB service sends contextual information, in the form of allowed certificate usage information that can help RPs to make an informed decision. The determination of this information can be obtained from the CP of the CA by the TB service and relayed as usage information to the RP. A context detector at the side of the RP can compare the actual application context with the usage information sent by the TB service without compromising the privacy of the user.

At a purely quantitative level, the TB service can send a score between 0 and 1 that represents the quality of the certificate, which we term the certificate level of assurance (CLoA). When the CLoA is 0, this indicates that the procedures followed by the CA to manage the subject certificates are very weak or non-existent. When the CLoA is 1, the applied procedures are very strong and faultless.

The TB service is able to handle all CAs regardless of their technical, geographic or legal situation, and may dynamically add new CAs to its database according to RP demand. The CLoA information may be complemented by another score that we call the confidence level (CL), which lies in the range from 0 to 1. This indicates the extent to which the TB service is confident about its CLoA score.

IV. Conclusion and Future Work

In this paper, we have analysed the existing trust approaches and shown than none of them meet the needs of RPs in the Internet. In on-going work, we have defined an algorithm for computing CLoA and CL values, and a protocol for transferring these between a web browser and trust broker. We have built a proof of concept TB service that we propose to validate by conducting experiments with users to demonstrate its impact and usability.

References

[1] Australian Government, "Gatekeeper PKI framework. Cross recognition policy," http://www.finance.gov.au/files/2012/04/Cross_Recognition_Policy.pdf, February 2009.

[2] Audun Jøsang, Ingar Glenn Pedersen, and Dean Povey, "PKI seeks a trusting relationship," In Proceedings of the 5th Australasian Conference on Information Security and Privacy, ACISP '00, pp. 191–205, London, UK, 2000.

[3] Microsoft, "Microsoft trusted root certificate: program requirements," http://technet.microsoft.com/en-us/library/cc751157.aspx.

[4] Mozilla, "Mozilla ca certificate inclusion policy," https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/, Version 2.2.

[5] William T. Polk and Nelson E. Hastings, "Bridge certification authorities: Connecting b2b public key infrastructures," http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/B2B- article.pdf, 2000.

[6] Federal public key infrastructure authority, "Criteria and methodology for cross-certification with the U.S. federal bridge certification authority," http://www.idmanagement.gov/sites/default/files/documents/crosscert_method_criteria_v3.0_0.pdf, 2012.

[7] Ahmad Samer Wazan, Romain Laborde, Francois Barrere, Abdelmalek Benzekri, and David W. Chadwick, "PKI interoperability: still an issue? a solution in the X.509 realm," In Information Assurance and Security Education and Training, volume 406 of IFIP Advances in Information and Communication Technology, pp. 68–82, July 2013.

[8] APEC TEL WG, "Achieving PKI interoperability," Technical report, APEC, 2001.