CYBERNETICA
Institute of Information Security

A Model for Automatically Evaluating Trust in X.509 Certificates

Abu Shohel Ahmed, Dan Bogdanov

T-4-11 / 2010

Abu Shohel Ahmed[1], Dan Bogdanov[1,2].
[1] University of Tartu, Institute of Computer Science
[2] Cybernetica, Institute of Information Security

The research reported here was supported by:

1. Estonian Science foundation, grant(s) No. 8124,

2. the target funded theme SF0012708s06 "Theoretical and Practical Security of Heterogenous Information Systems",

3. the European Regional Development Fund through the Estonian Center of Excellence in Computer Science, EXCS, and the Software Technology and Applications Competence Centre, STACC,

4. EU FP7-ICT project VirtualLife (contract no. 216064).

Cybernetica research reports are available online at
`http://research.cyber.ee/`

Mailing address:
AS Cybernetica
Akadeemia tee 21
12618 Tallinn
Estonia

A Model for Automatically Evaluating Trust in X.509 Certificates

Abu Shohel Ahmed, Dan Bogdanov

September 29, 2010

Abstract

Currently, X.509 certificates are the de facto standard for verified identification of a person or entity on the Internet. As more and more people and organizations are using X.509 certificates to prove their identities in online transactions, the reliability and trust level of certificates come into question. X.509 certificates are based on public key cryptography such as the RSA scheme. However, the certificate granting process is based on the certification policy of the certification authority. Non-conformant issuing policies turn the trust evaluation of a certificate into a subjective matter which creates a lack of interoperability among certificates and certificate authorities. This paper presents a model for evaluating trust in X.509 certificates. Our model considers extended certification fields, rating services and certification policy formalization methods to find a good way for determining the trust level of a single certificate.

1 Introduction

A Public Key Infrastructure (PKI) allows the identification of a subject based on user credentials. This is achieved by using certificates, in which a Certificate Authority (CA) asserts the association between an entity and its attributes. Usually, the CA issues a certificate to an entity based on its own guideline documents such as the Certificate Policy (CP) and Certification Practice Statement (CPS). The certificate policy file defines a set of rules that the CA maintains during the life cycle of a certificate. This is an important document to measure the trust level of a certificate. In addition, the certification practice statement states how the CA actually implements the certification policy during its operational time.

The certification mechanism only provides information regarding the validity of a certificate issued by a CA. However, there is no automated mechanism for verifying the trust level of a certificate. The main obstacles for certificate trust evaluation are non-machine-readable certification policies and certification practice statement document and also the measurement of CA trust. The objective of this paper is to measure the trust level of a certificate and to automate that process. There are several steps to measure certificate trust level:

1. correctness of a certificate
2. usage of extension fields
3. matching policy identifier with requirement
4. policies defined in the certification practice statement
5. the actual practice of the certification authority.

In this paper, we devise a stepwise solution using the above techniques. Our solution also focuses on semi-formalizing the CPS document which allows other parties to rate the CPS document automatically. In addition, we will focus on a fallback system based on blacklisting or rating of certificates.

The paper is inspired from the VirtualLife (VL) identity management system [1, 2] which is based on X.509 certificates. In VL, the strength of an identity is defined in three categories:

1. completely identified
2. weakly identified
3. not identified

We present a technique for determining the category for a certificate. The rest of the paper is organized as follows: Section 2 describes the certification process and the internals of an X.509 certificate, Section 3 describes the problems with X.509 certification, Section 4 describes previous studies in this area and Section 5 describes our proposed solution.

2 Certification and the X.509 certificate

A digital certificate is a digital document that certifies that a certain public key is owned by a particular user [3]. This document is digitally signed by a third party called the Certificate Authority to authenticate that the public key belongs to the certificate user.

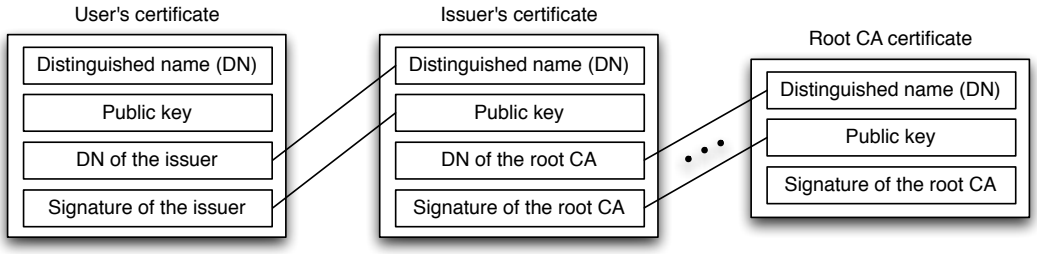

Figure 1: An example of a certificate validation path

2.1 The certification process

The first part of the certification process is the issuing of a certificate to an entity. To apply for a digital certificate, a certificate signing request (CSR) is sent from an applicant to a certificate authority. To generate a CSR, the applicant creates a public/private key-pair. The CSR also contains identifying information about the applicant. For example, the distinguished name, e-mail address and information about location or occupation. This information is signed by the applicant using the private key. The resulting CSR is then sent to the certificate authority who verifies the provided identity information of the applicant. If the request is successful, the certificate authority sends back the signed identity certificate to the applicant.

The certification authority is free to set up the policy of verifying actual identities. Some certification authorities operate in a completely online fashion. The authority can verify the user's access to an e-mail account and no other information. For domain certificates, the authority can require that the applicant can access the administrator e-mail account of that domain. However, in order to issue a more trusted certificate, the certification authority should verify the identity of the individual by requiring official documents and maybe even personal presence.

A valid certificate can be used to prove the identity of a person or any other entity. In a two-party authentication process, the receiving party can check the authenticity of a certificate using certificate path validation process. The certificate path is a list of certificates used to authenticate an entity. Figure 1 shows a typical certificate validation path [4]. Certificate validation is done in two steps. First, the party that relies on the certificate verifies the certificate and its signer using the certificate path. If the certificate is trustworthy for the relying party, it accepts the certificate. Second, the certificate is checked using a certificate revocation list (CRL) or an Online Certificate Status Protocol (OCSP) server to check the revocation status of a certificate. The CRL is a list of revoked certificates published by the certificate signer (CA). OCSP is similar in purpose to a CRL but provides an interactive online service for each request [5].

2.2 The X.509 certificate

The design goal of X.509v3 [6] is to support a wide range of applications and environments. It incorporates several extension fields to support the design goal.

2.2.1 Basic fields

The most basic fields that make up the certificate are described below.

`tbsCertificate:` This field contains the names of the subject and the issuer, a public key associated with the subject, a validity period, and other associated information.

`signatureAlgorithm:` The `signatureAlgorithm` field contains the identifier for the cryptographic algorithm that is used to sign the certificate.

`signatureValue:` The `signatureValue` field contains a digital signature of `tbscertificate`.

Some other fields in this group include the version number and the serial number. Figure 2 provides an example certificate with basic fields.

2.2.2 Certificate extensions

A X.509 certificate contains a series of certificate extensions fields. At a minimum, applications conforming to X509 version 3 must recognize the following extensions: key usage, certificate policies, subject alternative name, basic constraints, name constraints, policy constraints, extended key usage, and inhibit any-policy [6]. Among these extensions, three extensions are important for measuring trust of a certificate. These extensions are key usage, certificate policies, and policy mappings.

`Key usage`: The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key for a certificate [6]. The extension field is obligatory for certificates that contain public keys which are used for validating digital signatures on other public key certificates or CRLs.

`Certificate policies`: The certificate policies extension contains a sequence of one or more policy information terms, which are identified by an object identifier (OID) and optional qualifiers. For an end entity certificate, these policy information terms indicate the policy under which the certificate has been issued and the purposes of the certificate. Applications with specific policy requirements check a list of policies which they will accept and compares the policy OIDs in the certificate with the list [6]. Figure 3 shows a policy extension field.

`Name constraints`: This constraint restricts CA to issue only a certain type of certificate.

`Extended key usage`: This extension usually appears in end entities' certificates. If a certificate contains both a key usage extension and an extended key

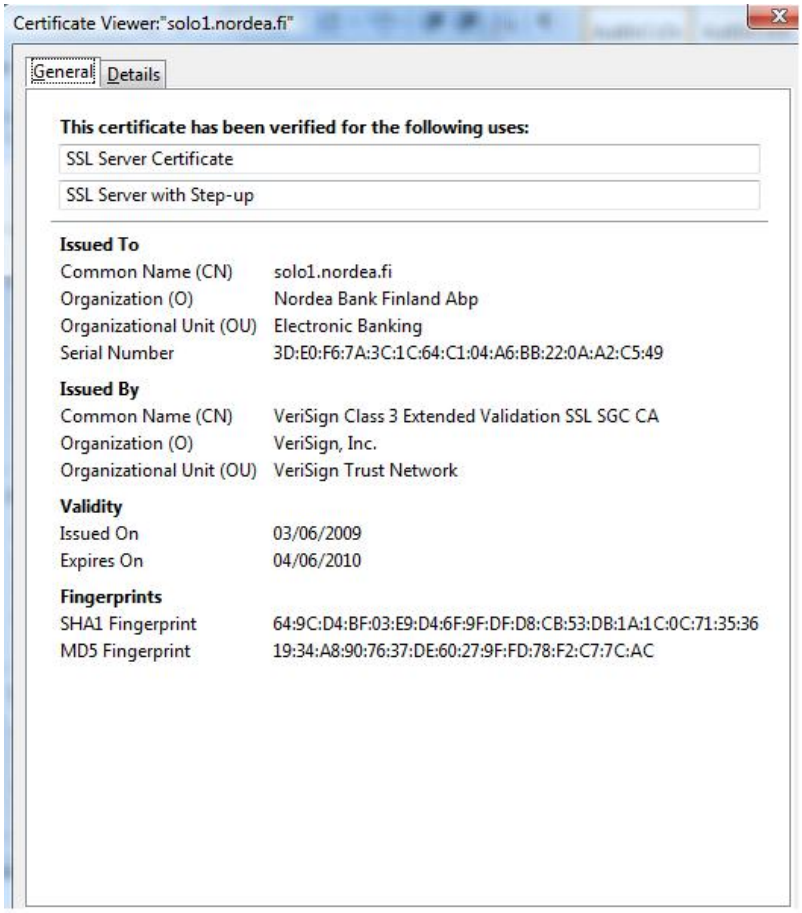

Figure 2: An example certificate in web browser

usage extension, then both extensions must be processed and the certificate must only be used for a purpose consistent with both extensions [6].

2.2.3 Extended validation certificates

Extended validation certificates (EV) is a special type of X.509 certificate that requires more extensive investigation of the requesting entity from the certification authority. Only certain number of CAs which follow the guidelines [7] can issue extended validation certificates. An EV clearly differentiates between low-validation certificates and rigorously validated certificates. Current browsers such as Internet Explorer 7, and Firefox 3.5 can easily identify EV certificates and provide user-friendly notifications in the address bar. For example, an EV certificate can be shown with green bar with subject name to help the user to identify the

```
[1]Certificate Policy:
    Policy
Identifier=2.16.840.1.113733.1.7.23.6
    [1,1]Policy Qualifier Info:
        Policy Qualifier Id=CPS
        Qualifier:
            https://www.verisign.com/rpa
```

Figure 3: Certificate policy field

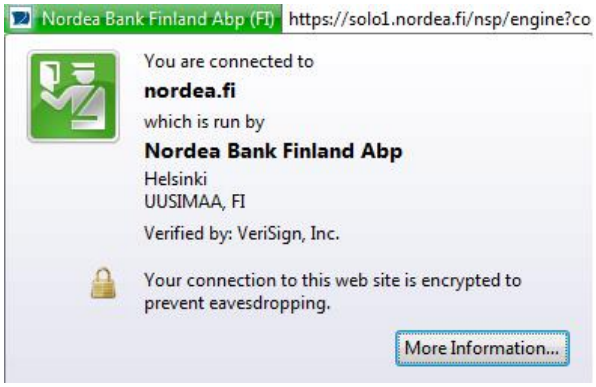

Figure 4: EV certificate in Firefox

entity. Figure 4 shows an example of an EV certificate in the Firefox web browser.

According to the extended validation guidelines, certificate authorities are assigned a specific EV identifier which is registered with the browser vendors. For example, the EV object identifier for Verisign is 2.16.840.1.113733.1.7.23.6 [8] which is tagged with certificate policy extension field of a X.509 certificate. The certificate policy field also includes a link to the CA's policy file (CPS). A client application which wants to evaluate the trust level of a certificate can verify the object identifier of a certificate with the published object identifier. The client application can also look into the corresponding CPS document to measure the trust level. In addition, a certification authority providing EV certificates must also provide an OCSP service to check the revocation status of a certificate. This enables client applications to check the revocation status of an EV certificate online.

2.2.4 Logotype

The logotype (RFC 3790 [9]) was introduced as a certificate extension field to provide visual or audio information about the subject of a certificate which aims to

help a human user to verify the certificate. Usually, a link is added to the logotype field of a certificate to access the user image or audio. Certificate authorities are obliged to put a valid image of the subject in the logotype field. This opens up a new opportunity to check the certificate using biometric or visual information of a subject. Although, this field is less popular at the time of writing this paper, it could be a vital measure for certificate identification.

2.3 Certificate authenticity and certificate class

The degree of trust in a certificate differs according to the class of a certificate. Usually, each CA has a policy to classify the certificate based on the trust level and identification mechanism. According to the VeriSign CPS, there are three classes of certificates based on trustworthiness [8]. Table 1 lists the VeriSign certificate classes.

Class 1	This certificate does not provide identity authentication. Only the email address of the subscriber is checked during the certificate issuing process.
Class 2	This certificate is issued based on authenticated data of a valid identity proofing service such as a credit bureau or another reliable source.
Class 3	A class 3 certificate is provided on personal presence of the certificate applicant or a document of notarization. This check also includes government certified documents such as identity cards or passports.

Table 1: VeriSign certificate classes

3 Problems with X.509

Although X.509 is a popular standard for certificate representation, it still lacks in certain areas. First, users use an undefined certification request protocol to obtain a certificate which is published in an unclear location [10]. Second, revocation is either handled in an ad hoc manner or ignored entirely. There is no standard technique to update revocation information to the end client. In addition, revocation should revoke the capabilities not the identities [10]. Third, certificates are based on owner identities not on some unique keys. Owner identities do not work very well in practice. For example, people can change their affiliation or email

address and thus, the identity information changes and the certificate will contain incorrect information.

3.1 Problems with X.509 CA policies

There are several problems associated with the CA policy. At present, a CA policy mainly serves three purposes [10]:

1. it provides a CA-specific mini-profile of X.509
2. it defines the CA terms and conditions and indemnifies the CA
3. hides kludges for PKI problem areas.

In addition, CA policies may define

1. obligations of the CA (e.g., check certificate user validity, and publish certificates/revocations)
2. obligations of the user (e.g., provide valid, accurate information, protect the private key, and notify the CA on private key compromise)

The CA policy file is the single most important document for measuring the trust level of X.509 certificates [10]. However, CA policy files are not homogenous across all CAs. The non-homogenous CA policies create problems in automatic evaluation of trust in a certificate. To overcome this policy differentiation, closed PKI models are introduced. For example, FPKI: (US) Federal PKI profile requires certain extensions (e.g, `basicConstraints`, `keyUsage`, `certificatePolicies`, `nameConstraints`) to be critical. This enables inter-operability and reliability between certificates when other vendors maintain the same level of X.509 extensions.

In X.509, the originality of the certified data lies completely within the restrictions of the policy management of a CA. This means that identity validation is performed within the framework of the CA using its own rules defined by the Certification Practice Statement. Thus, any deviation or lack of trustworthiness in the CPS creates a lack of trust in all the certificates signed by that CA.

4 Previous work

Several studies have been conducted to define a set of rules for evaluating the trustworthiness of a certificate and hence evaluating the certification policy of a CA. Omar and Lindsay [11] proposes a set of requirements for certificate evaluation. They have analyzed the policies of three CAs (EuroPKI, SwuPKI and DutchGrid)

to find a common criteria set which can be used to evaluate the trustworthiness of a subject. They finally propose 27 criteria to measure the trustworthiness of a subject in a certificate.

Stephan Grill [12] proposes description logic (DL) to formalize the Certificate Practice Statement document. The author also proposes a structured CPS mechanism using description logic. In order to integrate such a structured CP/CPS in a PKI system, several relevant aspects are presented in his paper: a suitable syntactic representation, a mechanism to bind such a structured CP/CPS to a certificate, alternatives for the relying party to specify requirements for acceptable policies and consequences for cross-certification [12].

A similar approach is used by Weaver [13] to define a semi-formal method to automate the trustworthiness decision of a CPS document. As US federal law states that CPS documents should be human readable, they propose a semi-formal method using XML for converting CPS documents defined by RFC 2527 and RFC 3647. They designed three tools—`PKI PolicyRepository`, `PolicyBuilder`, and `PolicyReporter` to automate this task.

The `PKI PolicyRepository` stores certificate policies for retrieval by their reference structure such as the object identifier. The tool segments a CPS document according to the style defined in RFC 3647 and stores it in a reference format. The second tool, `PolicyBuilder` assists the CA for creating policies based on `PolicyRepository`. The final tool, `PolicyReporter` helps the users by providing higher quality information during policy comparison. This tool searches the policy file for some keywords. Policy statements with the highest importance contain the words MUST, REQUIRED, or SHALL, the next most important provisions contain SHOULD or RECOMMENDED, and the least significant requirements use MAY or OPTIONAL [12]. The program counted this word in a file and indicates the trust level of a certificate. A large difference in word counts indicate discrepancies in the requirement levels of two sections of different policy files.

The Platform for Internet Content Selection [14] is an effort of the W3C to provide a technical means for users to select and reject websites based on the content [14]. The PICS architecture which consists of three components is shown in Figure 5.

The architecture consists of rating services and rating systems, labels and rules. A rating service is an individual, group, organization, or company that provides content labels for information on the Internet. The labels are based on a rating. When a user accesses a document, he at the same time checks the rating within the service. Based on the rating, it performed content categorization of the document.

Table 2 shows a comparison of approaches to the problem of certificate trust evaluation.

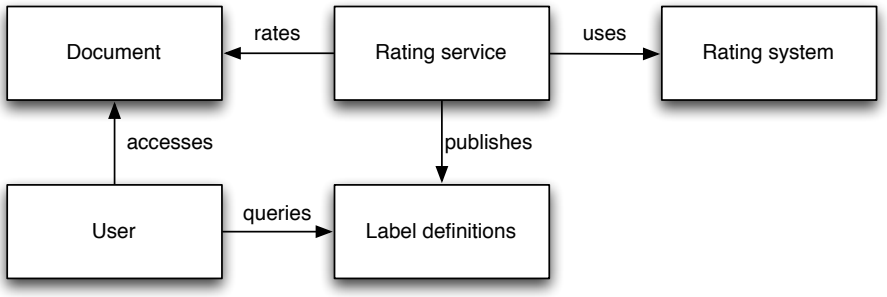

Figure 5: The PICS architecture

5 Proposed solution

The trust evaluation of a certificate is a complex process. As discussed previously, there are several techniques to achieve this objective. One option is to check the certificate extension fields and match those with the client application's policy requirement for a specific policy object identifier. Second, certificates are issued under a certificate policy and certification practice statement which are critical for trustworthiness of a certificate. Thus, the formalization or semi-formalization of the CPS document can enable the automatic trust measurement of a certificate. In addition, manual auditing by a trust body is necessary to check that a CA is following the CPS guideline during the certification life cycle. PKI audits verify that the certificate policies and certification practice statements are consistent with a framework of requirements. For example, the financial services industry has defined the ISO 21188 standard which specifies such requirements for banks and similar institutions. Other similar requirement standards include WebTrust and ANSI X9.79 [15].

Our proposed solution suggests several techniques to determine the trust of a certificate. The solution is based on the assumption that X.509 and the PKI model are the standard method for certification.

Step 1: Verification extension in X.509. We believe that a unified certificate verification extension field in X.509 format would significantly benefit the cause. This field would define the degree of verification the CA has performed to grant this certificate. `Meta-Certificate Group` has already proposed a field which contains nine categories according to the verification level [16]. Applications requiring a certain level of trust could consult this field to measure the trust level of a certificate.

Step 2: Semi-formalization of the CPS document. In this approach, the client application will fetch CPS documents specified in the policy extension field and

Solution	Advantage	Disadvantage
CPS semi-formalization	Processing is performed using local knowledge which means that applications can independently evaluate a certificate.	Trust evaluation is based on weak assumptions (e.g., counting words) which gives a less accurate result. Requires network access for requesting the CPS file.
CPS formalization	Provides more accurate information about the CPS file.	CPS files have no common standard. Requires network access for requesting the CPS file.
Ratings service	Flexible and easy to find rating for a certificate. Provides a clear direction about a certificate.	Trust depends on the independent auditing authority. Requires an online request to get the latest rating information.

Table 2: A comparative analysis of CPS trust evaluation techniques

analyze the CPS file using some available approaches (eg the one presented by Weaver [13]). This analysis can provide a valuable determination matrix for the client application regarding CA policy and trust level.

Step 3: The creation of a CA rating service. A rating service is a common approach for getting quality content from the Internet infrastructure which is distributed in nature. One solution is to create an online rating service based on the PICS architecture which provides a rating (e.g, trust level) for a CA and the associated machine-readable policy file. The ratings are provided by an independent auditing authority which verifies the integrity level of a CA and CPS document. We acknowledge, that CA evaluation is a subjective matter and a rating service creates another party to trust. However, we stress that the rating service just provides a user-friendly layer of simplification on top of the standard X.509 infrastructure. Users can still override the ratings with their personal trust preferences.

The proposed architecture of the rating service is shown in Figure 6. A description of the architectural components follows.

Benchmark body: The benchmark body is an independent body which states the set of trust requirements the auditing authority measures during the CA evaluation process. We can generate the trust requirements using the approach defined by Omar and Lindsay [11]. In addition, a common evaluation grade is determined

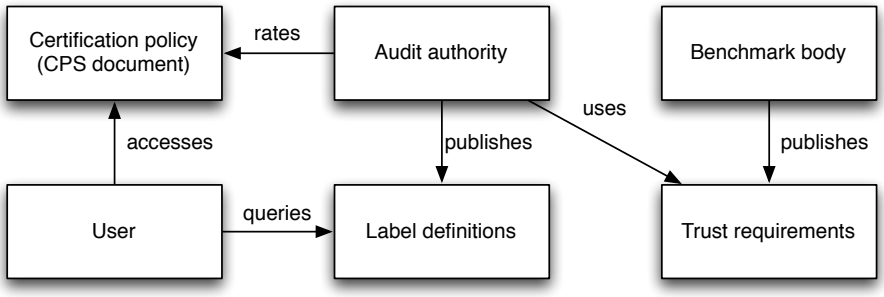

Figure 6: The certificate policy rating system

by this body. For grading, we can use the recommendation by MCG [16].

Audit authority: The audit authority evaluates the CA and its CPS documents according to a fixed set of criteria defined by the benchmark body. The audit authority also evaluates the actual practice of a CA in accordance with the published policy file. It assigns a label to each CA and associated policy file. The assigned label contains timestamp information, rating authority information and the actual rating. The rating is provided against each criteria defined by the benchmark body. Rating against each criteria enables the client application to measure trust according to its specific requirement. Timestamp information ensures the liveliness of audited data.

User applications: A client application first accesses the online service to get an associated label marking for a specific certificate. Second, it contacts the audit authority to get the published label definition. Finally, the trustworthiness of a CA and CPS is measured using ratings and label definition.

The rating architecture is distributed in nature with many online service providers and audit authority providers. The client application or users are free to choose the service provider whom it will trust. This can be solved similarly with the domain name system. Local caches of the ratings database can be kept on devices with no permanent network connection.

The CA evaluation process based on the PICS architecture also has several problems. The main problem is the dependency of the client application to the PICS server. This partially disables the offline verification of X.509 certificates, but we note that a similar problem has not stopped people from using OCSP. Furthermore, with this approach, small certification authorities that are not audited, will get a default ranking. Besides, there could be a disagreement between government controlled CA and the independent auditing body regarding data protection, policy and privacy issues of a CA.

5.1 Certificate trust evaluation

In many cases, client applications require automated or semi-automated trust evaluation of a certificate. A good example is an online virtual world like VirtualLife where user interacts with others in real time to perform business activities or social communication. The proper identification of the partner is vitally important for any business transaction. However, for a naive user, it is difficult to understand the difference between a more trustworthy certificate and a less trustworthy certificate. That is why the current browsers are shipped with the certificates of CAs deemed trustworthy for user guidance.

However, this guidance process may yield unintended results as the certification policies of the trusted root certificates are significantly different. We propose a new model for certificate trust evaluation. The complete trust evaluation process for certificates is shown in the flow diagram on Figure 7. The model is based on a rating mechanism that uses several sources. Finally, the accumulated ratings are compared against thresholds to evaluate the trust level of a certificate. The model is designed to work in line with the VirtualLife identification system which has three classes of trust in identity certificates [2].

The evaluation process is as follows. First, the client application maintains a data store of trusted and untrusted certificates. The data store contains extended validation certificates and previous knowledge base of trusted or un-trusted certificates. When a client application wants to evaluate a certificate, it checks its own data store to get the status of a certificate or the one of the signer of the certificate. If the certificate is in the trusted zone, it is accepted. On the other hand, if the certificate is in the untrusted zone, it is rejected. Users can manually add an unknown certificate to the trusted or untrusted data store.

However, if the certificate status cannot be evaluated from the data store, our model requires additional verification steps to automatically evaluate the trust level of a certificate.

Second, the system can check if the key usage field matches with the usage requirements of the client application. If the usage requirements matches the desired usage then continue with the evaluation. Otherwise, the certificate should be rejected if it is used for different purposes than required in the application.

Third, the application assesses the amount of information available in the certificate's distinguished name (DN) field. Certificates with less attribute information get a lower rating.

In the fourth step, the application checks the availability of the policy identifier and CPS link field. A certificate without a CPS link is considered as a low trust certificate.

In the fifth step, the application can use the semi-formalization technique on the CPS document to evaluate the trust level of a CA. Techniques presented by

Weaver [13] could be used for this purpose. A rating is provided based on this evaluation.

The sixth step provides uses the PICS model for CA and CPS rating to take into account a third-party evaluation of the certificate.

Based on the overall rating and threshold values, a certificate can be accepted, weakly accepted or rejected as a source of trusted information. Although our solution contains many steps, performing all of these steps are not necessary to achieve the trust goal. Rather all these steps can be seen as a combined approach for trust evaluation of a certificate.

6 Conclusion

This paper presents a guideline for measuring the trust level of a certificate. We have shown a combined approach which includes certificate extension fields, formalization of CPS and rating service to measure the trust level of a certificate. However, a client application only goes through the steps which are necessary to fulfill its demand for trust level. The presented model is quite robust to measure the trust level in a true manner for different types of certificates.

References

[1] "VirtuaLife Project." [Online]. Available: http://www.ict-virtuallife.eu/

[2] D. Bogdanov and I. Livenson, "VirtualLife: Secure identity management in peer-to-peer systems," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 40, 2010, pp. 181–188.

[3] B. Sotomayor, "Certificates and certificate authorities - chapter 10. fundamental security concepts." [Online]. Available: http://gdp.globus.org/gt3-tutorial/multiplehtml/ch10s04.html

[4] IBM, "IBM WebSphere(R) MQ information center." [Online]. Available: http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/index.jsp?topic=/com.ibm.mq.csqzas.doc/sy10600_.htm

[5] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP." IETF, June 1999. [Online]. Available: http://www.ietf.org/rfc/rfc2560.txt

[6] R. Housley, W. Polk, W. Ford, and D. Solo, "RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 3280, April 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3280.txt

[7] "Guidelines for extended validation certificates." [Online]. Available: http://www.cabforum.org/

[8] VeriSign, "VeriSign EV CPS v. 3.3." [Online]. Available: http://www.verisign.com/repository/CPS/VeriSignCPSv3.3.pdf

[9] C. Mickles and P. Nesser, "RFC 3790 Survey of IPv4 Addresses in Currently Deployed IETF Internet Area Standards Track and Experimental Documents." IETF, June 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3790.txt

[10] P. Gutmann, "Tutorial: Design and analysis of security systems." [Online]. Available: http://www.cs.auckland.ac.nz/~pgut001/tutorial

[11] O. Batarfi and L. Marshall, "Defining criteria for rating an entity's trustworthiness based on its certificate policy," in *Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), IEEE*, 2006.

[12] S. Grill, "Comparing and evaluating x.509 certificate policies and certification practice statements using description logics," in *MS Thesis, Institute for Applied Information Processing and Communication,Graz University of Technology*. [Online]. Available: http://arge.signaturen.at/downloads/Publikation.200112.pdf

[13] G. A, Weaver, S. Rea, S. W, and Smith, "A computational framework for certificate policy operations," in *Dartmouth College, Hanover, NH 03755, USA*. [Online]. Available: www.cs.dartmouth.edu/~sws/pubs/wrs09.pdf

[14] Resnick and P., "Filtering information on the internet," in *Scientific American*, 1997. [Online]. Available: http://www.sciam.com/0397issue/0397resnick.html

[15] R. Koorn, P. van Walsem, and M. Lundin, "Auditing and Certification of a Public Key Infrastructure," in *Information Systems Control Journal*, vol. 5, 2002.

[16] "The Meta-Certificate Proposal: Presentation Plan, 1997." [Online]. Available: http://mcwg.org/mcg-mirror/mcs97.htm

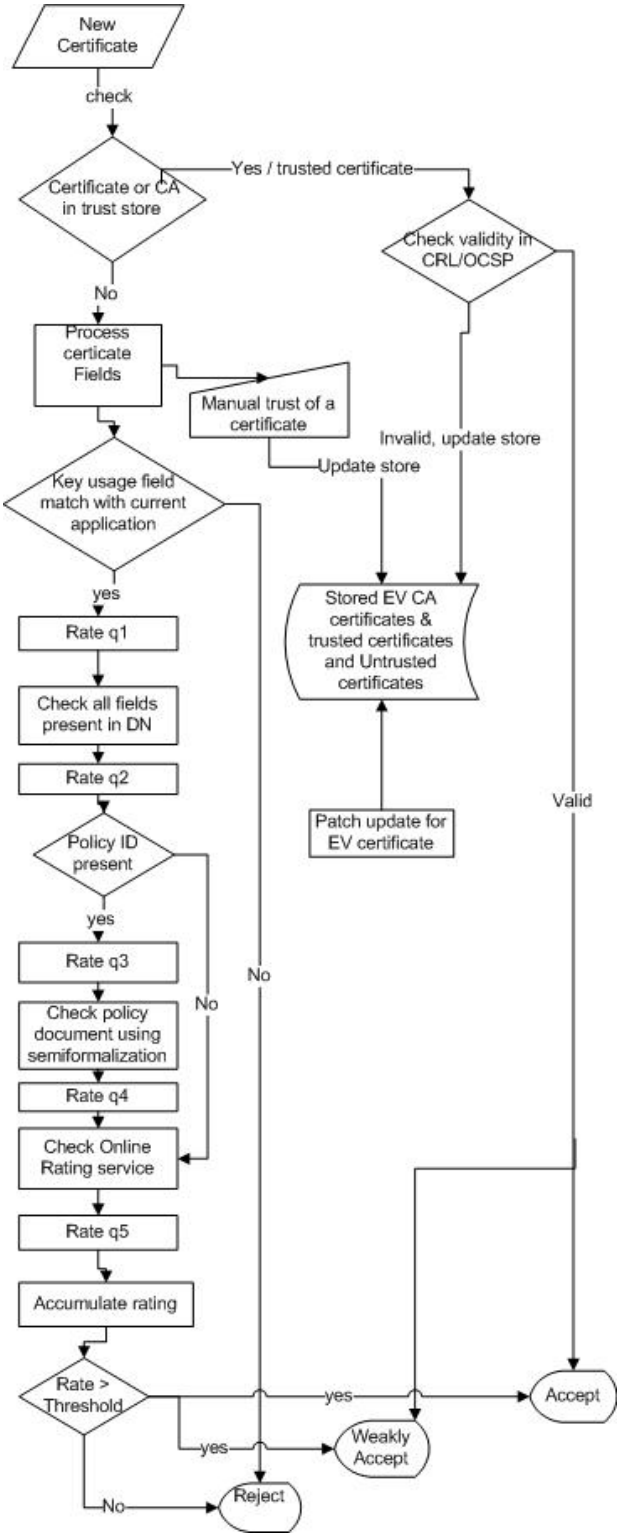

Figure 7: Proposed model of certificate trust evaluation