IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 3 Issue 11 November, 2015

Survey of X.509 Certificates Trust Evaluation

Miss. Varsharani Hawanna[1]; Prof. Dr. V. Y. Kulkarni[2]; Prof. R. A. Rane[3]

MIT, Pune, India.[1]; MIT, Pune, India.[2]; MIT, Pune, India.[3]

hawanna.varsha@gmail.com[1]; vrushali.kulkarni@mitpune.edu.in [2]; rashmi.rane@ mitpune.edu.in [3]

ABSTRACT

X.509 certificates are used to confirm the identity of the parties involved in the communication and to validate the information being transferred. Currently, more and more people and organizations are using X.509 certificates to prove their identities in online transactions, so the reliability and trust level of these certificates come into question. To solve this question in X.509 Certificates trust model many authors proposed their ideas in their research. In this paper we did survey of different research papers which help in giving answer to the question of X.509 certificates trust model and describe these papers in briefly with their advantages and disadvantages. We also describe the terms and concepts comes in understanding of x.509 certificates.

Keywords: X.509 trust model; X.509 certificate; certification authority; PKI, Chain of trust, Certificate Policy, Certification Practice Statement.

1. INTRODUCTION

We X.509 Public Key Infrastructure, an ITU-T standard for PKI. Formerly issued on July 1988, works hand-in-hand with the X.500 standard. It is used to confirm the identity of the parties involved in the communication and to validate the information being transferred.

It create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption [1]. It is a critical security mechanism as it is the cornerstone of major security services used in our daily life such as SSL, IPSec, XML signature, etc.

The X.509 trust model includes three entities: the certification authority (CA), the certificate holder (CH) and the relying party (RP). The CA is a trusted third party between the certificate holder and the RP. If certificate holder wants to communicate with RP, he/she/it have give the confirmation of it's identity, so certificate holder request for a certificate to CA. CA issues a certificate to certificate holder based on its own guideline documents such as the Certificate Policy (CP) and Certification Practice Statement (CPS). Certificate policy (CP)[2] is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. Certification Practice Statement (CPS) [2] is a statement of the practices which a certification authority employs in issuing certificates.

In summary, CA guarantees to the RP the correctness of the certificate holder's certificate information (certificate holder name, public key, certificate usage, etc.) by appending its signature to the certificate. This approach would be efficient if only one CA existed or at least RPs had a preexisting relationship with all the CAs. However, the current situation is largely different. Most of RPs has no relation with any CAs at all, and each CA has its own procedures and policies to manage certificates. As a result, RPs have to build their trust decision by performing several checks: the signature on the certificate has to be verified, the certificate status has to be verified, a path from the certificate to a trusted root certificate has to be discovered and evaluated, the extensions have to be checked etc. and most important RP have to analyze a set of documents like Certificate Policy (CP) and Certification Practice Statement (CPS). These are the important document to measure the trust level of a certificate. RP have to answer many technical and legal questions like what happens when a CA does not correctly check the identity of the certificate holder or when it issues deliberately 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? [3].

We did survey of papers in which authors describe their ideas to help RP in analyzing a set of documents for answering many technical and legal questions.

The rest of paper is organized as follows. Section II describe about background, particularly about one of the reasons for X.509 Certificates comes in picture. Section III describes about the terms and concept require in understanding of x.509 certificate. Section IV present In brief Literature survey. Section V contains conclusion.

2. BACKGROUND

2.1 Cryptography

It is the science and art of transforming messages to make them secure and immune to attack [4]. A cryptographic system consists of four essential components:

Plaintext – the original message to be sent.

Cryptographic system (cryptosystem)or a cipher – consisting of mathematical encryption and decryption algorithms.

Ciphertext – the result of applying an encryption algorithm to the original message before it is sent to the recipient.

Key – a string of bits used by the two mathematical algorithms in encrypting and decrypting processes

Two types of cryptography:

1. Symmetric key cryptography: uses only one secrete key for both encryption and decryption of the data. So it can be easily compromised.

Two solve problems of Symmetric key, Asymmetric key cryptography comes in picture.

2. Asymmetric key cryptography: It uses two different keys for the encryption and decryption of data. Sender encrypt message using public key of Receiver and Receiver decrypt using its own private key. The keys are generated in such a way that it is impossible to derive the private key from the public key, but the problem occurred during public-key encryption is Man_in_middle attack. Now, we will see what is Man_in_middle(MIM) attack.

2.2 Man_In_Middle Attack

In Man_in_middle attack [5], the attacker gets in the middle of the communication between two authenticate parries. Both sender and receiver think that they are communicating to each other but all the traffic goes through man which sit in middle between these two. To protect from this attack, digital certificates used.

2.3 Digital Certificates

A digital certificate [6] also called public key certificate[6] or identity certificate[6] which certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made by the private key that corresponds to the certified public key. In this model of trust relationships, a CA is a trusted third party – trusted both by the subject (owner) of the certificate and by the party relying upon the certificate, It issues digital certificates.

Digital certificates are used for Authentication, and authentication is the process of confirming an identity. In the context of how a network interacts, authentication involves the confident identification of one party by another party.

X.509 [7] specifies, standard formats for public key certificates or digital certificate.

3. X.509 Certificate

An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate. It specifies, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm**[7].**

3.1 Standard X.509 Certificate Format

It have 3 versions. Version1 include basic fields as shown in figure 1, version 2 include version1's all fields and additional issuer and subject unique identifier fields as shown in figure 1, but it is not widely deployed in the Internet therefore, version3 comes with additional extension fields, as shown in figure 1. Certificate Authority (CA) can use extensions to issue a certificate only for a specific purpose e.g. only for **signing digital object.**

In all versions, the serial number MUST be unique for each certificate issued by a specific CA [7].

Version: This field indicates the X.509 version of the certificate format (1, 2, or 3), with provision for future versions of the standard.

Serial Number: This field specifies the unique, numerical identifier of the certificate in the domain of all public key certificates issued by the Certification Authority (CA). When a certificate is revoked, it is actually the certificate serial number that is posted in a certificate revocation list signed by the CA It is for this reason that the serial number for each certificate in the domain must be unique.

Signature Algorithm: This field identifies the algorithm used by the CA to sign the certificate. The algorithm identifier, which is a number registered with an internationally-recognized standards organization (e.g., ISO), specifies both the public-key algorithm and the hashing algorithm (e.g., RSA with MD5) used by the CA to sign certificates.

.

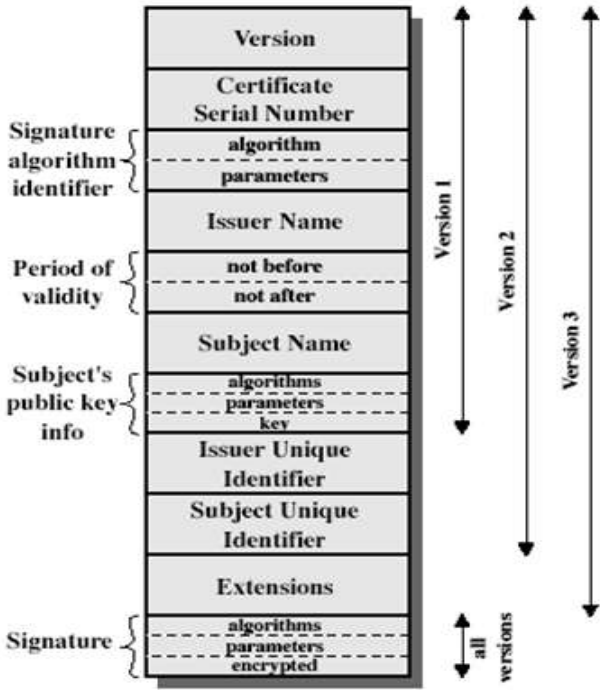

Fig 2. X.509 standard certificate format

Issuer X.500 Name: This field specifies the X.500 distinguished name (DN) of the CA that issued the certificate.

Validity Period: It specifies the dates and times for the start date and the expiry date of the certificate. Every time a certificate is used in Entrust, the software examines the certificate to ensure it is still within its validity period.

Subject X.500 Name: This field specifies the X.500 distinguished name (DN) of the entity holding the private key corresponding to the public key identified in the certificate.

Subject Public Key Information: This field identifies two important pieces of information: a) the value of the public key owned by the subject, and b) the algorithm identifier specifying the algorithm with which the public key is to be used. The algorithm identifier specifies both the public-key algorithm and the hashing algorithm (e.g., DSA with SHA-1).

Issuer Unique Identifier (version 2 only): This field was added to the X.509 certificate definition as part of the version 2 standard. The field, which is optional, provides a location to specify a bit string to uniquely identify the issuer X.500 name, in the event that the same X.500 name has been assigned to more than one CA over time.

Subject Unique Identifier (version 2 only): This field was added to the X.509 certificate definition as part of the version 2 standard. The field, which is optional, provides a location to specify a bit string to uniquely identify the subject X.500 name, in the event that the same X.500 name has been assigned to more than one subject over time.

Authority Key Identifier: This field specifies a unique identifier of the key pair used by the CA to sign the certificate. This identifier aids in the process of verifying a certificate signature in the case where a CA has used multiple key pairs in its lifetime.

Subject Key Identifier: This field used to identify the particular key pair associated with the public key in the certificate. This field is useful when a user has updated his key pairs (both signing and encryption) multiple times during his existence in the CA security domain. In such a case, the subject key identifier field is most useful when a user is attempting to decrypt a file encrypted for him with a public key that is not his current encryption public key.

Key Usage: This field specifies the intended use(s) of the key. The following list represents the settings for the key usage field: nonrepudiation, certificate signing, CRL signing, digital signature, key Encipherment, data Encipherment, key Agreement, encipher Only, decipher Only.

Certificate Policies: The CP field specifies the policies under which the certificate was issued to the user and/or the types of uses applicable to the certificate. Certificate policies are represented by specially-formatted numbers, known as object identifiers, which are registered with an internationally-recognized standards organization. It is possible to designate a number of certificate policies within a certificate. If the certificate policies field is set to be non-critical, the CA indicates which policies apply to the certificate, but is not requiring the certificate to be limited in use to situations only in accordance with those policies. If the field is flagged as critical, the CA is specifically limiting use of the certificate to situations in accordance with the policies

Subject Alternative Name: This field specifies one or more unique names for the certificate subject. The permissible name forms are as follows: Internet e-mail address, Internet domain name, Internet IP address, X.400 e-mail address, EDI party name, Web uniform resource identifier, any other name type with a recognized object identifier The purpose of these additional name forms is to support applications, and it is not the same as the user's X.500 distinguished name.

Issuer Alternative Name: This field specifies one or more unique names for the CA. The permissible name forms are

the same as those for the subject alternative name field, as above.

Basic Constraints: This field identifies whether the subject of the certificate is a Certificate Authority (CA) and how deep a certification path may exist through that CA. The pathLenConstraint field is meaningful only if CA is set to TRUE. In this case, it gives the maximum number of CA certificates that may follow this certificate in a certification path. A value of zero indicates that only an end-entity certificate may follow in the path.

Policy Constraints: This field is used in cross-certificates. The field specifies the set of acceptable policies in a certificate chain extending from a cross-certificate. It also specifies whether or not all certificates in a chain must meet a specific policy.

3.2 X.509 Sample certificate

Following is the certificate of IDBI bank issued by Entrust CA

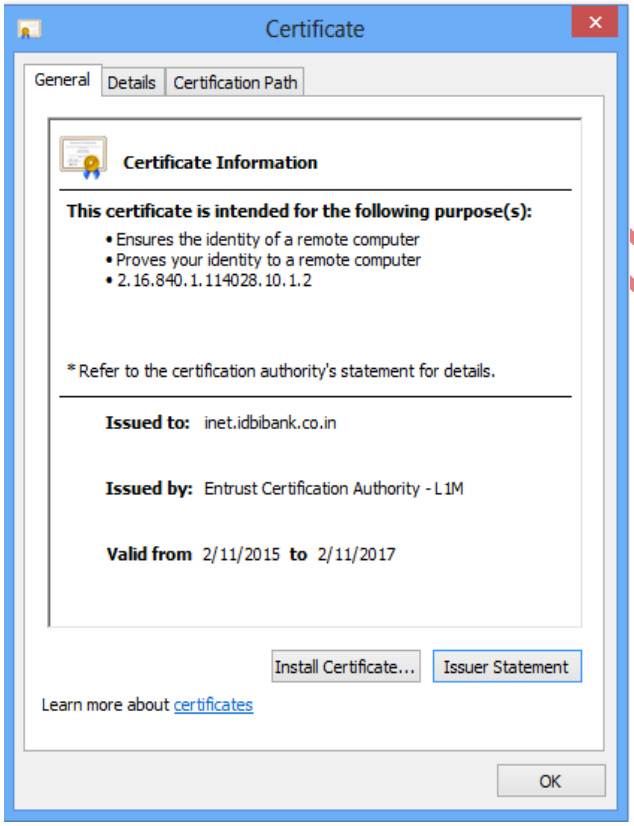

Fig 2: General Tab of sample certificate

Common certificate file extensions are:
.cer, .der, .pem(Base64 encoded certificate, enclosed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"), .p7c, .p7c [7]

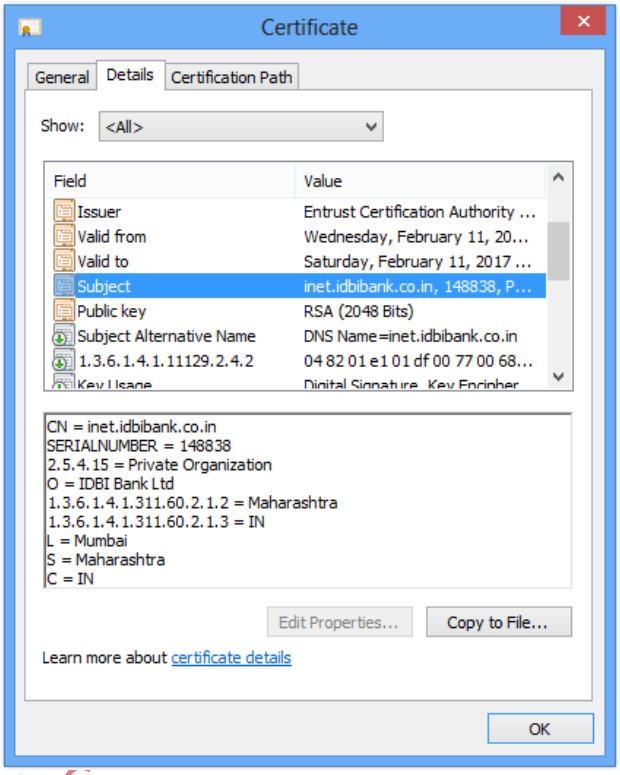

Fig 3: Detail Tab of sample certificate

3.3 Certificate Policy and Certificate Practice Statement

Crowd The X.509 standard defines a certificate policy as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements" [2].

The term certification practice statement (CPS) is defined by the ABA Guidelines as: "A statement of the practices which a certification authority employs in issuing certificates" [2].

Relationship between certificate policy and certification practice statement is like CPS is a detailed statement generally be more detailed than certificate policy definitions. Indeed, CPSs may be quite comprehensive, robust documents providing a description of the precise service offerings, detailed procedures of the life-cycle management of certificates, but a detailed CPS does not form a suitable basis for interoperability between CAs operated by different organizations. Rather, certificate policies best serve as the vehicle on which to base common interoperability standards.

A CA with a single CPS may support multiple certificate policies [2].

As described in section I RP have to analyze these two documents during trust evaluation, so we will see outline of a CPS proposed by RFC 2527 [2].

CPS content has eight components, which can be further divided into subcomponents, and a subcomponent may comprise multiple elements.

These are briefly described below:

1. Introduction:

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which the specification is targeted.

2. General Provisions

This component specifies any applicable presumptions on a range of legal and general practices topics.

3. Identification and Authentication

This component describes the procedures used to authenticate a certificate applicant to a CA or registration authority (RA) prior to certificate issuance. It also describes how parties requesting rekey or revocation are authenticated. This component also addresses naming practices, including name ownership recognition and name dispute resolution.

This component has the following subcomponents:

3.1. Initial Registration;

3.2. Routine Rekey;

3.3. Rekey after Revocation;

3.4. Revocation Request.

4. Operational Requirements

This component is used to specify requirements imposed upon issuing CA, subject CAs, RAs, or end entities with respect to various operational activities.

5. Physical, Procedural, and Personnel Security Controls

This component describes non-technical security controls used by the issuing CA to perform securely the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

6. Technical Security Controls

This component is used to define the security measures taken by the issuing CA to protect its cryptographic keys. It also be used to impose constraints on repositories, subject CAs and end entities to protect their cryptographic keys and critical security parameters. It do Secure key management.

This component consists of the following subcomponents:

6.1. Key Pair Generation and Installation;

6.2. Private Key Protection;

6.3. Other Aspects of Key Pair Management;

6.4. Activation Data;

6.5. Computer Security Controls;

6.6. Life-Cycle Security Controls;

6.7. Network Security Controls;

6.8. Cryptographic Module Engineering Controls.

7. Certificate and CRL Profile

This component is used to specify the certificate format and, if CRLs are used, the CRL format. Assuming use of the X.509 certificate and CRL formats, this includes information on profiles, versions, and extensions used.

8. Specification Administration.

This component is used to specify how this particular certificate policy definition or CPS will be maintained

3.4 Certification Authority Hierarchy

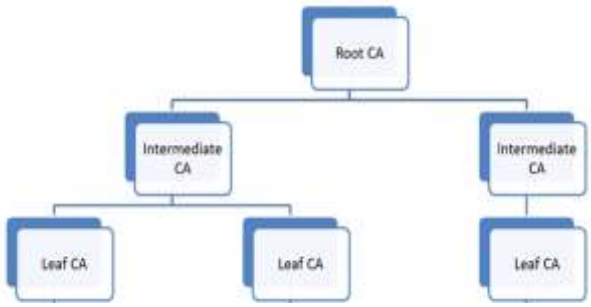

Fig 4: Certificate Authority (CA) hierarchy

The Root CA: It is the topmost Certificate Authority (CA) in hierarchy. The root CA provides certificates for intermediate CAs. The certificates can be revoked if they are compromised.

Intermediate CAs: It is a CA that is subordinate to another CA and issues certificates to other CAs in the CA hierarchy.

Leaf CAs: Leaf CAs are used to provide certificates to users, computers, and other services. There can be multiple issuing CAs, and one leaf CA can be used for generating computer certificates and another can be used for generating user certificates.

. 3.5 Chain of trust verification

Each X.509 certificate has an "issuer" field that contains the name of the certificate authority (CA) that issued the certificate. The certificate presented by the server i.e. leaf certificate here, should be accompanied by the certificate of the issuing CA and, if the issuing CA is not a root CA, the certificates of higher-level CAs all the way to a root CA [11].

For more detail refer RFC 5280.

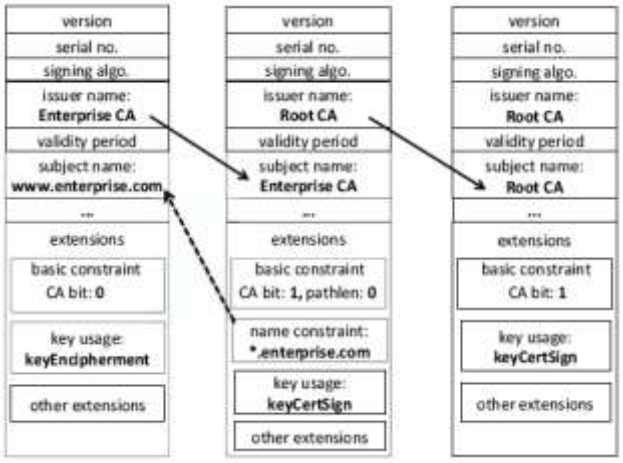

Fig 5 : A sample X509 certificate chain.

4. LITERATURE SURVEY

Place As the objective of this paper is to find out previous work done by authors to help RP in evaluating the trust of certificate presented by certificate holder. To fulfill this we did survey and comes up with some papers in which author proposed there idea to evaluate trust of certificate. In survey we found that some papers help RP by providing expert system which evaluate the trust of CA, while some paper evaluate trust of certificate itself, some paper formalize CP and CPS in a format that supports the implementation of automatic trust decisions. Brief descriptions of these papers are as below:

In paper [3], authors proposes an explicit expert recommender whose activity is to provide the necessary information allowing RPs to make an informed decision (the RP can understand why is (s)/he accepting or not a certificate for a particular transaction) about a CA. This new entity should be independent of PKIs and must play both the role of technical and legal expert for helping the RPs. By including explicitly this role to X.509 trust model, the task of RPs is simplified, and RPs need to rely only on the expert and not on each and every CA of certificate holders. In this case, the X.509 trust model is fairer for the RPs. The expert evaluates objectively the CAs and sends recommendations to RPs for helping them make informed decisions about certificates.

Advantage: Solution used in both situation when RP knows CA and when RP don't knows CA

In paper[12] authors proposed a solution which is based on the assumption that X.509 and the PKI model are the standard method for certification. Author uses Verification extension in X.509, Semi-formalization of the CPS document, CA rating service in there system and then evaluate the system as follows. First, the client application maintains a data store of trusted and untrusted certificates. When a client application wants to evaluate a certificates, it checks its own data store to get the status of a certificates or the one of the signer of the certificates. If the certificates is in the trusted zone, it is accepted. On the otherhand, if the certificates is in the untrusted zone, it is rejected. Users can manually add unknown certificates to the trusted or untrusted data store.

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

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 certificates 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 certificates. In the fifth step, the application can use the semi-formalization technique on the CPS document to evaluate the trust level of a CA. 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 certificates. Based on the overall rating and threshold values, certificates can be accepted, weakly accepted or rejected as a source of trusted information. All these steps can be seen as a combined approach for trust evaluation of certificates.

Advantage: Provide a ternary recommendation regarding certificates trustworthiness, not binary.

In paper[13],authors designed three tools: PKI PolicyRepository, PolicyBuilder, and PolicyReporter to automate task of finding trust level of Certificates. 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. The program counted this word in a file and indicates the trust level of a certificate. A CA whose Policy statement contains more most significant word, leads to more trustworthy.

Advantage: Processing is performed using local knowledge which means that applications can independently evaluate a certificate.

Disadvantages: Trust evaluation is based on weak assumptions (e.g., counting words) which gives a less accurate result. It requires network access for requesting the CPS file.

In paper [14][15], authors proposed a framework to provide RPs qualitive information to determine the Quality of Certificate (noted QoCER). This value is calculated based on two parameters: the QoCPS and the QoPKI. relation between QoCER, QoPKI and QoCPS as following:

$$QoCER = \Psi(QoPKI) \times QoCPS \quad (1)$$

where function Ψ can be any function that returns a result between 0 and 1, QoPKI is a value between 0 and 1, QoCPS is a value between 0 and 1.

In the framework, author proposes a process of validation which integrates the concept of QoCER First, system performs Classic search for the certificate of root authority. If this certificate belongs to the static trust domain, the RP accepts the certificate. The static trust domain contains fully known and controlled CAs. This allows enhancing the performance of the validation process when dealing with well known partners. Otherwise, the RP computes the QoCER that consists in:

a) Getting the QoCPS from a authority recognized to perform this task;

b) Getting the QoPKI of the CAs that has issued this certificate from an authority recognized to perform this task;

c) Computing the QoCER according to the specific function Ψ; . This quality represents a quantitative assessment of the authenticity and trustworthiness of the certificate.

Advantage: The value of QoCER being a discrete value, it makes users able to accept certificates depending on the criticality of the service they want to access. This implies that users can now specify the risk they want to take when they accept a certificate which was not possible before.

In Paper[16], describes a system that allows the trust index of a Certification Authority (CA) to be computed based on a CA's published Certificate Policy (CP) and Certification Practice Statement (CPS),At the heart of the system is an expert system that has knowledge about the factors that are important in computing the trust in a CA. the expert system asks the same questions to a CPS Server, which takes its answers from an XML formatted CPS. This requires the CA administrator to first produce an XML formatted CPS, which authors describe, and publish this in its LDAP directory along with its public key certificates and revocation lists. We describe the CPS server, which retrieves the XML CPS's as signed attribute certificates, and feeds answers to the questions posed by the expert system using a Simple SOAP protocol.

In paper[10], the main Objective of this paper is to represent Certificate Policies (CP) and Certification Practice Statements (CPS) in a format that supports the implementation of automatic trust decisions. so author proposes a structured CPS mechanism using description logic. In order to automate this process, author developed a system in the following steps:

1. A format (syntax and semantics) has to be defined to represent a CPS.

2. The textual CPS has to be translated into this structured CPS format.

3. The structured CPS has to be bound to a certificate.

4. The relying party queries this CPS.

5. The relying party specifies a local policy.

Advantages: Provides more accurate information about the

CPS file.

Disadvantage: CPS files have no common standard. Requires network access for requesting the CPS file

5. CONCLUSION

X.509 certificates have been largely adopted today by many people and organizations for proving their identities in online transactions, so the reliability and trust level of

these certificates come into question i.e. in x.509 trust model RP have to evaluate trust of certificate. To solve this many author proposes solutions to help RP, we review these solution and describe them in briefly with advantages and disadvantages.

6. ACKNOWLEDGMENTS

We thank Prof. Mr. B. M. Patil, Associate Professor, Department of Computer Engineering, MIT, Pune for sharing his pearls of wisdom with us and for his comments that improved the manuscript. We also express our sincere thank to all the authors, whose papers in the area of spam filtering are published in various conference proceedings and journals, and to all authors and organizations of referred websites.

7. REFERENCES

[1] Wikipedia contributors. Public Key Infrastructure(PKI) [online]. Available:https://en.wikipedia.org/wiki/Public_key_infrastructure

[2] S. Chokhani, CygnaCom Solutions,Inc., Ford W., VeriSign,Inc, "Certificate Policy and Certification Practices Framework", RFC 2527, March 1999.

[3] A.S.Wazan, R. Laborde, F. Barrère, A. Benzekri, "The X.509 trust model needs a technical and legal expert", IEEE, 2012, pp. 6895-6897.

[4] William Stalling, "Cryptography and Network Security-Principles and Practice", *in Prentice-Hall India*, 3rd ed. USA.

[5] Wikipedia contributors. (2012, January). Man_In_Middle Attack. [Online]. Available:https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[6] Wikipedia contributors. Public Key Certificate [online]. Available:https://en.wikipedia.org/wiki/Public_key_certificate

[7] Wikipedia contributors. X.509 [online]. Available: https://en.wikipedia.org/wiki/X.509

[8] Ian Curry, "Version 3 X.509 Certificates", Entrust Technologies White Paper,1998.

[9] Ralph Holz, Lothar Braun, Nils Kammenhuber, Georg Carle, "The SSL Landscape – A Thorough Analysis of the X.509PKI Using Active and Passive Measurements",ACM, 2011.

[10] 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,2001, [Online]. Available: http://arge.signaturen.at/downloads/Publikation.200112.pdf

[11] Chad Brubaker, Suman Jana, Baishakhi Ray, Sarfraz Khurshid, Vitaly Shmatikov, "Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations", IEEE, 2014, pp.114-119.

[12] Abu Shohel Ahmed, Dan Bogdanovin, "A Model for Automatically Evaluating Trust in X.509 Certificates", in University of Tartu, Cybernetica, T-4-11 / 2010,pp.12-16. [online]. Available: http://cyber.ee/uploads/2013/05/T-4-11-A-Model-for-Automatically-Evaluating-Trust-in-X509-Certificates.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,2009,[Online]. Available: www.cs.dartmouth.edu/ sws/pubs/wrs09.pdf.

[14] Wazan,Laborde,Barrère,Benzekri, "Validating X.509 Certificates Based on Their Quality", IEEE, 2008, pp.2055-2060.

[15] A.S. Wazan, R. Laborde, F. Barrère, A. Benzekri, "A formal model of trust for calculating the quality of X.509 certificate," Security and Communication Networks, Wiley, Vol. 4 N. 6, june 2011,pp.651-660

[16] E.Ball, D.W Chadwick, A. Basden," The Implementation of a System for Evaluating Trust in a PKI Environment", Information Systems Institute Salford, University of 2003,pp.1-12

[17] D.Cooper, NIST, S. Santesson, Microsoft, Trinity College Dublin,S. Boeyen, Entrust, R. Housley, Vigil Security, W. PolkNIST, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" RFC 5280, May 2008.