Calculating and Evaluating Trustworthiness of Certification Authority

Zakia El uahhabi, Hanan El bakkali

ENSIA, Mohammed V University, Morocco
{zakia.eluahhabi, h.elbakkali}@um5s.net.ma

Abstract: In a public key infrastructure trust model, a trust is transferred along a set of certificates, issued by certificate authorities (CAs) considered as trustfully third parties, providing a trust chain among its entities. In order to deserve this trustworthiness, a CA should to apply the rigorous procedures for generating keys, checking the identities, and following reliable security practices. Any deficiency in these procedures may influence its trustworthiness. In this context, some authorities could be weaker than others. Then, relying parties (RPs) need a mechanism to evaluate CA trustworthiness. In this paper, we provide them this mechanism to have information about its trustworthiness. In fact, we propose a trust level calculation algorithm that is based on three parameters which are the CA reputation, the quality of procedures described in the certificate policy and its security maturity level.

***Keywords*:** PKI, certificate authority, trust level, reputation, certificate policy, X.509 certificate.

1. Introduction

Public key infrastructure (PKI) is an effective technology for business activities and for security in distributed system. The trust propagation in a specific PKI depends on the PKI's syntactic trust structure which is commonly known as a trust model [1]. PKI trust model plays an important role in extending and managing trust relationships between different entities. It determines how and under which situations trust can be initiated and established in the PKI.

In this infrastructure, a certificate authority (CA) is a trusted-by-all party used for managing certificates [31]. It creates such certificates for its CHs and guarantees to relying parties (RPs) their identity.

However, each CA has its own practices for ensuring the validity of the identity indicated in the issued certificate. When these practices are not in compliance with its certificate policy (CP) and/or certification practice statement (CPS), the CA is considered to be untrustworthy. Furthermore, this authority can be attacked by hackers who succeed to access to its systems and generate false certificates. Also, there would be many possibilities for a malicious CA that issues and generate false signatures and false certificates. In addition, RP trusts a CA for the correctness of the binding between the information included in a certificate and the public key. Its decision about this accuracy depends on the reading of the CP/CPS. Also, CHs can download the CP/CPS in order to evaluate it and decide which policy satisfies their requirements.

Nevertheless, it would be practically difficult for RPs and CHs to judge the CP/CPS and they often do not have the expertise to audit the CA's adherence to the CP [1]. Then, RPs and CHs need an automated mechanism to evaluate CA trustworthiness. In our approach, we propose this mechanism which is used to determine its trustworthiness.

The objective of this paper is to calculate the CA trust level (TLoCA) and automate the trust decision making process. TLoCA value helps RPs to make decision about CA trustworthiness. For instance, when a RP receives a certificate signed by a specific CA, he needs to verify the correctness of the information contained in this certificate. Thus, he requests TLoCA of this CA from our system in order to accept or not a received certificate.

Its calculation depends on three parameters that are the CA reputation score, the certificate policy quality that represents the evaluation of the procedures described in the published CP, and its security maturity level that indicates the CA security which must be ensured in issuing certificates. We will give more details about these parameters and a method to calculate them in Section 5. Besides, this trust level can be increased or decreased according to the respective values that the parameters aforementioned take.

The rest of this paper is structured as follows. Section 2 reviews the related work. Section 3 contains the main PKI concepts. In Section 4, we analyze the trust framework architecture that we have designed. Section 5 presents our proposed trust level calculation algorithm. In Section 6, we present through an example how apply our approach for calculating a TLoCA. Last section concludes the paper and provides some research work directions.

2. Related work

There are several approaches have been proposed for a trust assessment in PKI. Among these approaches we highlight the following.

Maurer proposes [6] an approach for modeling and reasoning about a PKI from the RP view point. In this approach, a certificate issued by CA Y for user Bob can be used by Alice if and only if he knows the Y public key and is convinced of its authenticity. Thus, he trusts Y to be honest and to correctly authenticate the owner of a public key before signing it [6]. Maurer's model utilizes confidence values which present Alice statements about the authenticity of other entities' public key and its trustworthiness. They are interpreted as probabilities. In [7], the authors present another trust model for trust evaluation in PKI. They define a trust calculus used to derive trust between entities in a certification chain. However, these models do not indicate the trust factors which influence the CA trustworthiness.

The proposed approach of [9,14] approximates a real trustworthiness of CAs. The authors use a CertainTrust trust

model of Ries [8] for the management and establishment of an entity's trust view. This trust view contains collected information about the CAs that user encounter when browsing. They use a distributed reputation system for CAs in order to improve the information collection and thus, speed up the bootstrapping of trust views. This system aggregates the provided opinions for calculating an issuer trust recommendation, which is distributed to users helping them making trust decisions about a certificate. However, the proposed approach necessities a long time until a user has seen all required CAs, based on his browser history.

In [33], a framework has been presented to evaluate a risk level of X.509 certificate based on certain trust criteria and characteristics. They use classification techniques with machine learning algorithm, which classify a certificate risk in three levels as high risk, medium risk and low risk [33]. Their framework is divided in three modules: Module 1 is used for collecting a trusted and untrusted x.509 certificate and storing it in trust store, Module 2 permits to collect trust criteria/attribute that are taken into account during risk level calculation, and Module 3 is used for a risk classification. The proposed framework helps user to know the risk he wants to take when he accepts a certificate for a specific transaction.

The authors of [34] present a technique for advising clients of the trust level of CA by assessing the certificate issued by such authority. Then, they define a model for evaluating the certificate. In this model, a certificate authority trust service collects a set of certificates that have been submitted by users and evaluate them according to the rules based on different factors such as certificate validity, conflicts between the certificate and other certificates granted by the CA for the domain, the sequence of CAs back to a root CA and the certification techniques followed by the CA to grant the certificate [34]. Also, it generates a certificate authority trust set defining a CA trust level which is distributed to users. However, the collected certificates are submitted to the certificate authority trust service by clients that may be the malicious users. In this case, it cannot judge the CA based on these certificates. Also, the proposed approach necessities a long time until the certificates are collected and submitted by users in order to determine a CA trust level.

In order to evaluate a trust in a PKI environment, some researchers base trust evaluation on CAs' policies [5,10,11,12]. So, it is necessary to automate this processing by policy formalization. In general, such formalized policies are complex to be read and evaluated by the relying entities. Consequently, such approaches necessitate legal and technical experts to evaluate it. In [13], the authors define a new role of legal and technical expert into the X.509 trust model to assist the RP in making decision about the certificate information correctness. Each expert setup a validation service. When a RP asks about a certificate quality, this service sends him the certificate quality level which is calculated using the quality of CA and CP. The proposed solution is used in both situations when CA is unknown and when RP knows it. Based on predicate calculus, the approach of [5] considers PKI trust model from a global view. They formalize the trust relationships among PKI entities by taking into account constraints concerning certificate policies, certification path length and certification practices. In our point of view, the CA policy is not enough to perform a complete CA trust evaluation. There are others factors that affect its trustworthiness as security risk which is signaled in [1] and CA reputation as it is highlighted in [29].

Unfortunately, at our best knowledge, there is no approach that uses all these factors in the CA trust evaluation process. Thus, we propose a new approach that integrates and combines these factors in the evaluation process of CA trustworthiness, such as the CP as it is highlighted in [5,10], security risks and CA reputation. We note that the proposed evaluation process is done automatically. Then, we define an algorithm that calculates a CA trust level based on these factors. We will give more details about our approach in Section 4 and 5.

3. Main PKI concepts

Many PKI definitions are used in the literature. In this paper, we consider the one presented by American Bar Association [2]:"PKI is the sum total of the hardware, software, people, processes, and policies that, together, using the technology of asymmetric cryptography, facilitate the creation of a verifiable association between a public key (the public component of an asymmetric key pair) and the identity (and/or other attributes) of the holder of the corresponding private key (the private component of that pair), for uses such as authenticating the identity of a specific entity, ensuring the integrity of information, providing support for non repudiation, and establishing an encrypted communications section". Generally, PKI allows users to enjoy the basic services of non repudiation, data integrity, confidentiality, and authenticity. It provides them the mechanism to communicate securely and establish trust relationships through the certificate use. The CA is the main entity of this infrastructure. It is responsible for registering and issuing, revoking, updating and generally managing certificates [2,32].

3.1 Certificate

The certificate is an electronic document contained the public key and personal data of its holder. Generally, it contains the issuer identifier, the expiration date, the subject identifier, and its public key. It is signed by the CA private key in order to confirm the correctness of the information included in the certificate. It is issued according to a certification policy.

Evaluation trust in a validated certificate can be defined as "the quality of the certification policy combined with the belief in the CAs adherence to that policy" [1]. The most widely used certificate format is the IETF X.509 standard.

Among certificates types we mention: identity certificates and attribute certificates [30]. Identity certificates verify that a public key belongs to an identity [26]. Attribute certificates do not contain the subject public keys. It can incorporate attributes that specify authorization information related to the CH [26].

3.2 Certificate policy and certification practice statement

In the system including a PKI, RP needs to be able to make trust decision about a CA for the information correctness included in a certificate. The decision about this accuracy depends on the procedures quality described in a CP/CPS, such as the procedure for protecting the CA private key, and

the registration procedures. The deficiency in one of these procedures may influence the CA trustworthiness.

A certificate policy, according to X.509, is defined as “a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements” [3]. Thus, the CP role is to assist a user in deciding whether a certificate is sufficiently trustworthy for a particular application [5].

More details of the practices followed by a CA in managing and issuing certificate are included in a CPS. According to the American Bar Association Digital Signature Guidelines, "a CPS is a statement of the practices which a certification authority employs in issuing certificates" [4]. In general, CPS covers the practices in particular procedures of a CA and especially those related to the issuing and management of public key certificates.

4. Proposed Trust Framework Architecture

Firstly, we will start with presenting an overview on the steps of the TLoCA calculation before giving details on the proposed trust framework architecture. Figure 1 shows these steps.

We have four steps for evaluating CA trustworthiness:

-Step 1: Calculating a reputation score (RepScore) based on the analysis of feedbacks given by CHs, a CP quality (CPQ) under which this CA operates, and its security maturity level (SLoCA).

-Step 2: Calculating a CA trust level (TLoCA) using the parameters aforementioned.

.

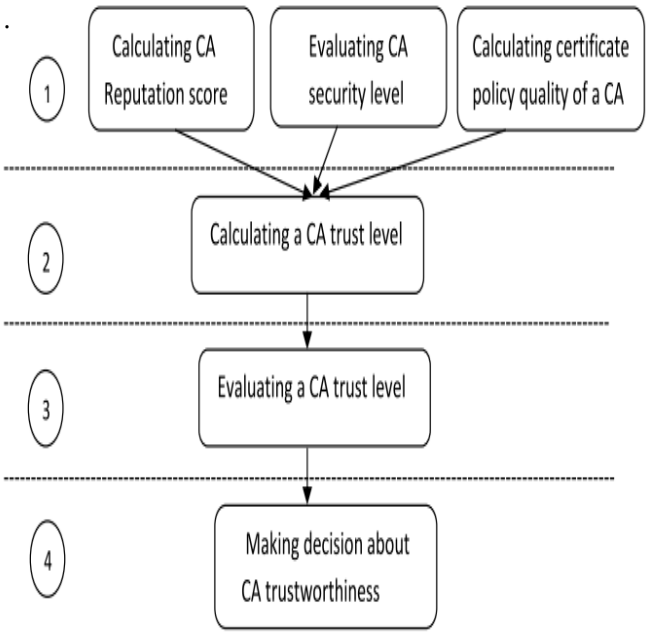

Figure 1. Overview of the proposed system

-Step 3 and step 4: Evaluating a TLoCA value helps RPs and CHs in making a trust decision about a specific CA when they ask for its trustworthiness.

Figure 2 illustrates the architecture of the proposed trust framework. This framework provides a means to obtain such a CA trust level. This level helps RPs to make decision about CA trustworthiness in order to accept or not a received certificate which is signed by such authority. It includes the various components involved in the TLoCA calculation. In the following, we explain these components:

- **CH interface**: An interface where CHs leave the feedback text and rating on the CA.
- **RP interface:** An interface used to request a TLoCA by RP.
- **Server:** It is responsible for calculating and evaluating a TLoCA. It consists of four components: the reputation module, trust module, CPQ module, and security module. This server could be managed by an independent trusted authority (TA).
- **Reputation module:** Once the CH rating is received by the module, it is stored in feedback database (DB), and then used by the reputation calculator to calculate/update the specific CA RepScore. Finally, the reputation calculator passes the calculated RepScore to the trust module for using it to compute a TLoCA and stores it in Reputation DB.
- **CPQ Module:** It includes two components: CPQ calculator and CPQ database (CPQ DB). The first calculates a CP quality using an algorithm for fetching information from the CP in XML format which will be defined in a future paper. It passes its value to the trust module. Also, the computed value is stored in CPQ DB.
- **Security Module:** It is composed of CA-SL Evaluator and SL DB. The first retrieves data from the SL DB and uses it to evaluate a CA SL. This data contains information, like CA software level EAL and its implemented security standard, collected by a moderator from trusted sources and stored in database (SL DB). We will aim to automate the information collection process in a future work.
- **Trust Module:** This module contains the trust calculator. Its role is to calculate a requested TLoCA value. Upon submission of a TLoCA request by a RP for a specific CA, the trust calculator sent its request to reputation module, CA-SL CA-SL module, and CPQ module asking them respectively the RepScore, the SLoCA, and the CPQ of a CP that is followed by such CA for issuing certificates. The provided parameters are used for computing a TLoCA. Finally, the calculated trust value will be sent to the RP.

The proposed framework can be accessed through an embed link into e-services applications such as e-commerce. We ask e-services users to provide their feedback on a CA that has issued them a certificate. However, some CHs are not interested in leaving their feedback. So, it is necessary to give them the incentives in order to increase the use of our framework and encourage them to leave their appreciations on a specific CA. For example, we could motivate the e-commerce users to provide their feedback by giving them an incentive such as having a chance to be included in a raffle and win a nice product. Also, we could explain them that their participation can be useful for making their trust decision about a particular CA in issuing a validate certificate.

5. Calculating RepScore, CPQ, SLoCA and TLoCA

Specifying the factors that influence CA trustworthiness is an important task for calculating its trust level. As mentioned previously, RPs trust a CA for the correctness of the binding between the information included in the certificate and the

public key. The correctness of the binding depends on the procedures quality which are followed by a CA and described in a CP. On the other hand, a CA reputation reflects the people's view on its behavior. Positive or negative reputation of this authority can have a great affect in making decision about its trustworthiness [25]. Furthermore, a CA security is an important factor which can influence trust decision. Any deficiency in the security of its systems can lead to generate false certificates. In the following subsections, we define and provide in details the calculation methods for the mentioned factors.

5.1 CA reputation score

We calculate a CA reputation on the basis of different feedbacks ratings provided by CHs. In order to compute RepScore, we use the exponentially weighted moving average (EWMA) method [15]. Roberts (1959) first described the use of EWMA control schemes [16]. This method weighs recent observations more and does not ignore old ones. In this manner, a reputation score is updated without ignoring its older value which reduces over time.

Also, this method can reflect the last tendency of CA reputation. On the other hand, shifts can be caused by intrusion or attack in computer network practice [17]. Then, EWMA control charts are usually used to detect smaller shifts [17]. Control chart is control limits which help in determining whether a process is in statistical control [18]. In this sense, this methodology is usually adopted to detect the malicious users [18,19,32].

Thus, we calculate a CA RepScore with the following:

$$\mathrm{Re}pScore = \alpha * rtg + (1-\alpha) * Old\,\mathrm{Re}pScore \quad (1)$$

Where,

RepScore: calculated reputation score

OldRepScore: old reputation score

$0 < \alpha \leq 1$: smoothing constant that defines the given weight to previous data. Selecting its value is a matter of personal preference and experience. In our case, if α has low value then old reputation has more influence. Its high value gives more weight to recent rating that influences reputation. As a result, we must choose a suitable α to control the strictness of our system. We propose to set α value between 0.6 and 0.7.

rtg: new rating given by a CH.

The center line for the control chart is the target value or $\mu 0$. The lower and upper control limits are:

$$UCL = \mu 0 + L * \sigma * \sqrt{\frac{\alpha}{2-\alpha}} \quad (2)$$

$$LCL = \mu 0 - L * \sigma * \sqrt{\frac{\alpha}{2-\alpha}} \quad (3)$$

Where,

L : is equal to 3 (the 3-sigma control limits) or chosen using the Lucas and Saccucci tables (ARL = 370)

σ : estimated variance computed from historical data (ratings received from CHs).

μ_0 : mean of historical data.

In general, a statistical anomaly is detected when the values fall outside the UCL or LCL. Hence, if RepScore value lies within the critical region (outside the UCL or LCL), the last user rating is considered malicious. In this case, its value will be ignored and not be taken into account in a RepScore calculation process. We note that values of UCL and LCL are changed according to new ratings that are received during a regular time interval.

The algorithm 1 hereafter describes the reputation score calculation. The function "repscore" gets parameters values which are discussed previously as input in order to use them in the RepScore calculus.

Algorithm 1. Reputation score calculation

Function repscore (idCA,α,rtg,oldrepscore,ucl,lcl,n)
Input : idCA id of a CA
α is a smoothing constant
rtg a list of new ratings received
oldrepscore the last reputation score of a CA
ucl is the upper control limit
lcl is the lower control limit
n is a threshold value
Output: newRepScore a calculated RepScore of a CA
1. We define the following variable:
m is a size of rtg
2. **For** i ← 1 to m
//initialise an oldScore value
3. **If** newRepScore value exists **then** //It is already calculated
oldScore ← newRepScore
4. **Else If** oldrepscore value does not exist **then**
//oldScore is initialized by a first rating
oldScore← rtg[1]/100
5. **Else** oldScore ← oldrepscore
6. **EndIf**
7. **EndIf**
newRepScore← α*rtg[i]/100 +(1-α)oldScore
8. **If (**m >= n**) then**
9. **If** ((newRepScore>ulc) or (newRepScore<llc)) **then**
//newRepScore lies within the critical region. In this case, its value will be ignored and not be taken into account in a calculation process
newRepScore ← oldScore
10. **EndIf**
11. **EndIf**
12. **EndFor**
13. **Return** newRepScore
14. End

In our algorithm, we apply the control chart methodology to detect the malicious ratings when the number of CHs, that leave their feedback, is representative and reaches a threshold value. This threshold presents the representative number of users which can be taken into consideration in calculating a TLoCA. It is determined using a Statistical Sampling Technique. We consider that this threshold equals to a sample size n representing the total user subpopulation that are certified by a same CA. We note that our population is the total number of the users that use e-services applications, into which a link of our platform is embedded. We divide members of this population into different subgroups (subpopulation) according to name of CA that certifies them. All members of each subgroup have been certified by a same CA.

Before defining the simplified formula for calculating a sample size, there are two terms must be explained. These are: precision level and confidence level. The first one, sometimes called sampling error, is the range in which the true value of the population is estimated to be [23]. This level is expressed in percentage (e.g., e=±5 percent). The second term means that a chance that the sample represents the true population value [23]. For example, selecting a 95% confidence level means that 95 out 100 samples would contain the true population value according to a certain level of precision. Most researches commonly use the 95% confidence level [23].

For calculating a sample size which represents our user subpopulation, we use a simplified formula [23], as follows:

$$n = \frac{N}{1 + N * e^2} \quad (4)$$

Where,

N: size of the user subpopulation.

n: sample size.

e: precision level (e=5%). A 95% confidence level is assumed for this Equation.

Furthermore, a CH can rate each CA, as explained in the previous section, by leaving her feedback. The provided rating is a number expressed as a percentage that is included in [0,100]. This rating provides information about how a CH appreciates the CA in question, as shown in Table 1.

Table 1. Explanation of the provided ratings

Rating	Explanation
[0,20]	Very bad
(20,40]	Bad
(40,60]	Moderate
(60,80]	Good
(80,100]	Perfect

Besides, the calculated reputation score values would be included in [0,1]. Also, UCL and LCL values belong to the threshold [0,1].

If the CA reputation is worst, its related score is then included in [0,0.2]. The bad reputation has a score included in (0.2,0.4].The moderate reputation is represented by a score belonging to the threshold (0.4,0.6]. Additionally, the good reputation score is included in (0.6,0.8] whereas the maximal value is for "perfect reputation" that is included in (0.8,1].

5.2 Computing the CPQ

Consulting a CP/CPS document permit to verify partially the CA trustworthiness but that is not sufficient. Most RPs never read the policies, and even if they did the policies would be difficult to interpret [1]. So, it would be practically difficult for RPs and CHs to judge the CP/CPS because it is very long and may be written by a language different from the user's language. For example, it may be written in French, thus it is not easy to read by people who do not understand French.

Also, it can contain the ambiguous terms which may be difficult to understand them by users. Consequently, there is a need for automating the CP interpretation process that can assist RPs and CHs in making trust decisions about a particular CA.

In this paper, we describe the automated process to judge the procedures announced in the published CP. In fact, we compute a CPQ indicating that these announced procedures are rigorous or weak. In this section, we present the process that we went through for calculating the CPQ. We define a CP tree structure based on a template standard of RFC 3647 [20].Within the framework of this RFC, a CP consists of components, that can be composed of subcomponents, and a subcomponent may contain multiple elements. The nine primary components proposed by RFC 3647 [20] are described below:

1. Introduction
2. Publication and repository
3. Identification and Authentication
4. Facilities, Management, and Operational controls
5. Technical Security Controls
6. Certificate Life-Cycle Operational Requirements
7. Certificate, CRL, and OCSP Profile
8. Compliance Audit
9. Other business and Legal Matters

The authors in [10] assign a weight value to various aspects of the policy. This assigned value defines the importance of that aspect comparing to other aspects [10]. In our approach, we calculate a score of each component. This score presents the importance of its content for calculating a CA trust level. We consider that the importance of each component is presented by its content.

Moreover, we compute the score value by using a scoring method. It is between 0 and 1. We assign a score to each element of subcomponent (elm_score) according to its content. Then, we compute a score of each subcomponent (subscore) by summing all the scores values of its elements and divide the result on the number of these elements (m). We use a same process for calculating a component score (score); we sum all the score values of its subcomponents and divide the result on a number of these subcomponents (n) (see Figure 3). For example, the component 6 'Technical Security Controls' as illustrated in Figure 3 consists of the eight subcomponents: 'key pair generation and installation', 'private key protection and cryptographic module engineering controls','time-stamping', etc. The subcomponent 'key pair generation and installation' comprises seven elements. Each element has a score. As a result, to calculate the CPQ, we sum all the calculated score values of the components (scorei) and divide the result on its number 9:

$$CPQ = \frac{\sum_{i=1}^{9} scorei}{9} \quad (5)$$

The score values, which are assigned to the subcomponent elements, are defined in table 2 as follow:

Table 2. Explanation of the assigned score

Score	Explanation
0	Weak
0.5	Medium
1	strong

The calculated CPQ values would be included in [0,1]. We classify the CP quality in three categories: high, medium and low quality. Thus, we use this threshold [0,1] and divide it into 3 subintervals equitably. If the CP quality is high, its values would be in (0.7,1].

The moderate quality is represented by a value belonging to the threshold (0.3,0.7]. Finally, the low quality value is included in [0,0.3]. In addition, the CP formalization is not detailed in this paper and will be discussed in a future paper.

Additionally, we use a XML language to represent a tree structure of a CP in digital form. The adjustment of the scores is determined according to an algorithm which is going to be detailed in a future work. The CPQ calculator applies this algorithm for computing CPQ. For example, for the element of the subcomponent "Key pair generation and installation", if a key pair is generated in hardware, an assigned score to this element is 1. A key pair generated in hardware might be more trustworthy than a key pair generated in software [24]. Also, for the element of key size, if CA's keys size for the RSA algorithm is at least 512 bits, its assigned score value is 0.

5.3 Evaluating a SLoCA

CA Security is a complex property that cannot be easily measured. CA system is vulnerable for any attack kind. Then, it has many security risks; CA's private key might be stolen or cracked. In fact, the attacker does not obtain a copy of its private key, but is able to use it for issuing a fraudulent certificate that violate various aspects of a CA security policy [21]. In addition, the attacker can also generate one or more signed false certificate revocation lists (CRLs). A fake certificate can allow attackers to send malicious emails in the name of others, enter classified web sites, or camouflage an E-Business web site [22]. In this case, the CA trustworthiness would be influenced by its security risks in e-services. For example, e-commerce depends on trusted CA to establish security between their services and users. When accessing a web site securely, a public key certificate is required to certify the web site identity. If the CA security is compromised, users trust in this e-service is negatively influenced. As a result, CA security is a factor that influences trust.

In order to protect the CA from security breaches, it is important that the CAs systems implement the highest security standard and are audited regularly to ensure their compliance with these security requirements. On the other hand, each CA uses software to generate public/private key pairs, issue the certificates, and manage the CRLs and life cycle of certificates. The evaluation assurance level (EAL) is an important factor to trust in the CA. In this sense, if the used CA software is certified by the Common Criteria Standard (CC), its security features are evaluated by establishing the EAL level. The CC lists seven levels: EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, and EAL7.These levels EAL5-7 describe high assurance. EAL3 to 4 are medium assurance levels. Also, the lowest level of assurance is between [EAL1-EAL2]. More details about these levels can be found in [27,28].

Thus, we evaluate a CA system security level on the basis of a combination between an implemented security standard and the CC level (EAL) provided for software used by this CA. In the table bellow, we show how we determine SLoCA values:

Table 3. Explanation of the assigned security maturity level (SLoCA)

EAL	Security standard	SLoCA	Explanation
[EAL1-EAL2]	-	0	Weak
[EAL1-EAL2]	ISO/IEC 27001	0.5	Medium
[EAL3-EAL4]	-	0.5	Medium
[EAL3-EAL4]	ISO/IEC 27001	1	Strong
[EAL5- EAL7]	-	1	Strong
[EAL5- EAL7]	ISO/IEC 27001	1	Strong

The SLoCA values are 0, 0.5, and 1 which represent weak, medium, and strong respectively. For example, we assign SLoCA =1 to a CA adopting the ISO/IEC 27001 which is a well-known information security standard published by the International Organization for Standardization and the International Electro-technical Commission. Also, EAL of the used software is one of these levels EAL5, EAL6, or EAL7. Moreover, a SLoCA value update depends on the changing of an implemented security standard or EAL.

5.4 Calculating a trust level TLoCA

TLoCA is quantitative information that measures and evaluates the CA trustworthiness. We calculate its value according to a CA reputation as well as its CPQ and its SLoCA. So, the aforementioned parameters are combined by the trust calculator using the weighted average method to compute a TLoCA value, as represented in equation 6:

$$TLoCA = \frac{w1 * \mathrm{Re}\, pScore + w2 * CPQ + w3 * SLoCA}{\sum_{i=1}^{3} wi} \quad (6)$$

We sum the parameters values multiplied by their respective weight (w) and divide the result on sum of these weights. w1, w2, w3 represent the weights which are assigned to each parameter and $\sum_{i=1}^{3} wi$ equals to 1. These weights represent the impact of these factors on the TLoCA.

A new TLoCA is calculated each time these parameters are changed. RepScore is updated when receiving new ratings during a regular time interval or the RP request about a TLoCA. CPQ and SLoCA seem to be constant. However, they can be updated when the security standard and the CA policy vary. Then, they are a same weight value (w2=w3). As a result, the weights adjustment depends on the impact of each parameter on TLoCA calculation process. This adjustment is determined in the following steps:

- Step 1: At the beginning, we may not receive any rating from CHs. In this case, the initial TLoCA is calculated with the following:

$$TLoCA = \frac{w2 * CPQ + w3 * SLoCA}{\sum_{i=1}^{2} wi} \quad (7)$$

Where,
w2=w3=0.5

$$\sum_{i=1}^{2} wi = 1$$

- Step 2: In this step, we can have a few CHs that use our framework and provide their feedback for a specific CA. In this case, we can't judge the CA reputation based on the low number of CHs. Hence, the weight value assigned to RepScore must be lower than that of CPQ and SLoCA. It is equal to 0.26.
- Step 3: When the CHs number increases and reaches a threshold value, computed by using an equation 4, we increment the weight value of RepScore (w_1=0.5). It will become higher than that of CPQ and SLoCA .

The algorithm 2 hereafter describes the TLoCA calculation. The calculated trust level would be included in a threshold [0,1].

Algorithm 2. Trust level calculation

Function trustlevel (idCA,RepScore,CPQ,SLoCA,n,k)
Input : idCA id of a CA
RepScore is a CA reputation score
CPQ is a CA certificate policy quality
SLoCA is a CA security level
n is a threshold value
k is CHs number that provide their feedback
Output: TLoCA is a CA trust level
1. If Repscore value does not exist **then**
TLoCA ← 0.5 ∗ CPQ + 0.5 ∗ SLoCA
2. Else If (k<n) **then**
TLoCA ← 0.26* RepScore+0.37* CPQ+ 0.37*SLoCA
3. Else
TLoCA← 0.5*RepScore+0.25*CPQ+ 0.25*SLoCA
4. EndIf
5. EndIf
6. Return TLoCA
7.End

There are four trust levels: no trust, low trust, medium trust, and high trust. The maximal value represents the case of "high trust" which belongs to the range (0.75,1], whereas the minimal value is for "no trust" that is included in [0,0.25]. Concerning, the case of "low trust", its values belong to the threshold (0.25,0.5], whereas the values which are included in (0.5,0.75] indicate that "medium trust".

6. Example

Our platform is useful to make decision about CA trustworthiness. Let us consider the following context:

- A RP receives a certificate signed by a specific CA. In order to accept or not the certificate, he looks for knowing the TLoCA of this CA. Then, he accesses our platform and requests its TLoCA value that helps him to make decision about the CA trustworthiness. Hence, he decides to accept or not a received certificate.

We explain through an example how the TLoCA value is calculated using our approach. Firstly, we suppose that the obtained CPQ of CA policy is 0.75 and this CA implements the ISO/IEC 27001. The CC level provided for software used by this authority is EAL4. We consider three scenarios:

- In first scenario, we suppose that CHs do not leave any rating for a CA. In this case, we calculate a TLoCA using two parameters CPQ and SLoCA. According to the table 3, the SLoCA value is 0.5. By applying the algorithm 2, we obtain the following result:

$$TLoCA = 0.5 * CPQ + 0.5 * SLoCA = 0.5 * 0.5 + 0.5 * 0.75$$

$$TLoCA = 0.625$$

The value 0.625 is included in (0.5, 0.75]. As a result, the trust level assigned to this CA is medium.

- In second scenario, we assume that some CHs use our framework providing their feedback for a CA in question. Supposing that we receive 50 ratings. In this case, we calculate a CA reputation score based on the received ratings, as shown in Table 4:

Table 4. Ratings Given by the CHs (expressed as a percentage)

CHs	Given Rating	CHs	Given Rating	CHs	Given Rating	CHs	Given Rating
CH_1	50	CH_{14}	73	CH_{27}	30	CH_{40}	50
CH_2	40	CH_{15}	50	CH_{28}	20	CH_{41}	35
CH_3	70	CH_{16}	45	CH_{29}	60	CH_{42}	45
CH_4	20	CH_{17}	65	CH_{30}	10	CH_{43}	70
CH_5	65	CH_{18}	60	CH_{31}	70	CH_{44}	60
CH_6	30	CH_{19}	30	CH_{32}	55	CH_{45}	75
CH_7	25	CH_{20}	50	CH_{33}	50	CH_{46}	50
CH_8	10	CH_{21}	65	CH_{34}	55	CH_{47}	55
CH_9	60	CH_{22}	75	CH_{35}	60	CH_{48}	30
CH_{10}	50	CH_{23}	70	CH_{36}	50	CH_{49}	65
CH_{11}	45	CH_{24}	40	CH_{37}	65	CH_{50}	55
CH_{12}	75	CH_{25}	50	CH_{38}	40		
CH_{13}	55	CH_{26}	60	CH_{39}	45		

First of all, we verify if CHs number reaches a threshold value or not. As mentioned in previous section, this threshold value is a sample size n representing the total user subpopulation. In this scenario, we suppose that the number of users that are certified by a same CA and use e-services application, into which a link of our framework is embedded, is 20 000 users. By applying the equation (4), we calculate the threshold value, as follows:

$$n = \frac{N}{1 + N * e^2} = \frac{20000}{1 + 20000 * 0.05^2} = 392$$

We conclude that the CHs number is lower than the threshold value n. Then, the weight value assigned to RepScore is 0.26. We use a weighting factor α=0.6. By applying the algorithm 1, we obtain RepScore=0.61. This value is computed from 50 ratings. It is included in (0.6,0.8]. As a result, the CA reputation is good.

By applying the algorithm 2, we calculate the TLoCA value. Then, we obtain the following result:

$$TLoCA = 0.26 * 0.61 + 0.37 * 0.75 + 0.37 * 0.5 = 0.62$$

0.62 belong to the threshold (0.5,0.75]. Consequently, the trust level of this CA is medium.

- In third scenario, we suppose that the CHs number is 400. It is more than a threshold value n. In this case, we apply the control chart methodology; we compute UCL and LCL from 400 ratings values by using the equations (2) and (3).The estimated variance which is calculated from users' ratings is 0.04 and $\mu 0 = 0.53$. Then, we obtain the following result:

$$UCL = 0.53 + 3 * 0.04 * \sqrt{\frac{0.6}{2 - 0.6}} = 0.61$$

$$LCL = 0.53 - 3 * 0.04 * \sqrt{\frac{0.6}{2 - 0.6}} = 0.45$$

By applying the algorithm1, the RepScore is updated. If its value lies within the critical region (outside the 0.61 or 0.45), the last user rating, which is used to compute this RepScore, is considered malicious. In this case, its value will be ignored and not be taken into consideration in a reputation score calculation process (see Algorithm1). The RepScore obtained is 0.59. We note that its weight value is 0.5 (400>n).

By using the algorithm2, we obtain the following result:

$$TLoCA = 0.5 * 0.59 + 0.25 * 0.75 + 0.25 * 0.5 = 0.61$$

0.61 is included in threshold (0.5,0.75]. As a result, the trust level of this CA is medium.

7. Conclusion

The objective of our work is to make RPs and CHs able to decide if a CA is trustworthy or not for issuing and managing public key certificates. In this paper, we propose a new approach on calculating and evaluating a CA trust level by combining the trust factors which are mentioned previously. We define a trust level algorithm attempting to calculate the CA trustworthiness value. It depends on three parameters that are the CA reputation score value as well as its CP quality and its security maturity level.

In future work, we aim to improve the TLoCA calculation process taking into account the certificates obtained by a CA that we evaluate its trustworthiness. According to [5], issuing a certificate by a trusted CA for another CA implicates that the issuer CA places certain trust in it. In this context, we will evaluate this implicit trust according to the issued certificate fields, which will be detailed and discussed in a future paper. Thus, a new trust level calculation for a CA will be added to the previous one. That will ameliorate the TLoCA calculation when receiving a low number of CHs. Also, we will focus on formalizing the CP and developing the algorithm for fetching information from the formalized CP in order to calculate a CPQ value. Finally, we will develop our approach and evaluate its effectiveness in our experimental.

References

[1] J.Audun, "PKI Trust Models," Theory and Practice of Cryptography Solutions for Secure Information Systems," ISBN 9781466640306, pp. 279-301,2013.

[2] PKI Assessment Guidelines of the American Bar Association, 2001,Available:http://www.americanbar.org/content/dam/aba/administrative/science_technology/pagv30.authcheckdam.pdf

[3] ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information technology, open systems interconnection-the directory: authentication framework", 1997.

[4] American Bar Association, "Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce", ISBN1-57073-250-7,1995.Available: http://www.americanbar.org/content/dam/aba/events/science_technology/2013/dsg_tutorial.authcheckdam.pdf

[5] E. Hanan and I.K. Bahia, "A predicate calculus logic for the PKI trust model analysis," IEEE International Symposium on Network Computing and Applications (NCA),New York ,pp.368 –371, 2001.

[6] M.Ueli, "Modelling a public-key infrastructure," ESORICS, Springer-Verlag, Vol.1146 , pp. 325-350,1996.

[7] H.Jingwei, and N.David."A calculus of trust and its application to PKI and identity management," The 8th Sympsium on Identity and Trust on the Internet, New York,pp.23-27,2009.

[8] S. Ries, S.M.Habib, M. M¨uhlh¨auser, and V. Varadharajan," Certainlogic: A logic for modeling trust and uncertainty (short paper)," published in Trust and Trustworthy Computing (Springer Berlin Heidelberg), Vol. 6740, pp. 254–261,2011.

[9] C.Jiska, B.Johannes, V.Florian, H. Matthias, and M .Max,"A Distributed Reputation System for Certification Authority Trust Management," 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communication s (IEEE UbiSafe Symposium), Finland, pp.1349 - 1356 , 2015.

[10] A.S. Wazan, R.Laborde, F.Barrere, and AM. Benzekri,"A formal model of trust for calculating the quality of X.509 certificate," Security and Communication Networks Journal, Vol.4 N. 6, pp. 651-665, 2011.

[11] L.Steve, and A .Carlisle,"Understanding PKI: concepts, standards, and deployment considerations". Second Edition, Addison-Wesley, pp. 11–15, 2003.

[12] G.A.Weaver, S.Rea,S.W.Smith, "A computational framework for certificate policy operations," 2009. Available: www.cs.dartmouth.edu/_sws/pubs/wrs09.pdf.

[13] S.W. Ahmad, L.Romain, B.François, and B.Abdelmalek, "The X.509 trust model needs a technical and legal expert," 12th IEEE International Conference on Communications (ICC), pp.6895 – 6900, Ottawa, 2012.

[14] B.Johannes, V.Florian, B. Johannes, and M. Max,"Trust views for the web PKI," In Public Key Infrastructures, Services and Applications, Springer, Vol 8341, pp.134–15, 2014.

[15] M.L.James and S.S.Michael, "Exponentially Weighted Moving Average Control Schemes: Properties and Enhancements. Technometrics," Vol.32, pp.1-12,1990.

[16] S.W.Roberts,"Control Chart Tests Based on Geometric Moving Averages," Technomearics," Vol. 42, No. 1,pp. 97-101,2000.

[17] Č.Petar and M.Č Sanja,"Optimization Methods of EWMA Statistics," Acta Polytechnica Hungarica, Vol. 8, No. 5, pp.73-87, 2011.

[18] V.V.Rajendran, and S.Swamynathan, "Hybrid model for dynamic evaluation of trust in cloud services," Wireless Networks, Springer, Vol.22, No.6, pp 1-12, 2015.

[19] S.B. Satyadeep and V. B.Vipul, "Recommendation System with Detection and Prevention of Malicious Feedback Rating," International journal of engineering sciences and research technology, Vol 3, No 1, 2015.

[20] S.Chokhani, W.Ford, R.Sabett, C.Merrill, and S.Wu, "Internet X.509 public key infrastructure certificate policy and certification practices framework," RFC 3647, 2003.

[21] K.Stephen,"Evaluating Certification Authority Security," IEEE Aerospace Conference, Vol.4, pp.319 – 327, 1998.

[22] L.Jingqiang,J.Jiwu, and L.Peng, "A Framework for Intrusion Tolerant Certification Authority System Evaluation," 26th IEEE International Symposium on Reliable Distributed Systems, Beijing, China, pp. 231-241, 2007.

[23] D.I.Glen,"Determining sample size,"1992. Available: https://edis.ifas.ufl.edu/pdffiles/PD/PD00600.pdf

[24] G.Stephan, "Modeling X.509 Certificate Policies Using Description Logics," Proceedings of the International Workshop on Applications of Description Logics, pp.86-93, Vienna, Austria, 2001.

[25] T.Oleena, and J.Sumy, "Literature Analysis on Reputation Models for Feedback in E-commerce," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, No 1, 2015.

[26] G.Mantas, D.Lymberopoulos, and N.Komninos, "PKI security in large-scale healthcare networks," Journal of Medical Systems, Vol.36, No 3, pp. 1107-1116, 2012.

[27] Common Methodology for Information Technology Security Evaluation - Part 3 Security Assurance Requirements, 2005. Available: https://www.commoncriteriaportal.org/files/ccfiles/ccpart3v2.3.pdf

[28] P.D.Ruben, "Requirements Engineering in the Information Assurance Domain: the Common Criteria Evaluation Process," the Springer International Series in Engineering and Computer Science, Vol.753, , pp.139-167, 2004.

[29] F.L.Yee, "Digital Signatures, Certification Authorities: Certainty in the Allocation of Liability," Singapore Journal of International & Comparative Law, Vol. 7, No 1, pp.183-200, 2003.

[30] Z.Eluahhabi, and H.El Bakkali,"A comparative study of PKI tr ust models", International Conference on Next Generation Net works and Services (NGNS),Morocco, pp.255 – 261, 2014.

[31] B.H.Sofiane, O.abdelkader, B. Asmaa,"Predictive preemptive certificate transfer in cluster-based certificate chain," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 6, No. 1, 2014.

[32] X.Wei, J.Fan, M.Chen, T.Ahmed, A. K. Pathan," SMART: A subspace based malicious peers detection algorithm for P2P systems," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 5, No. 1, 2013.

[33] V.Hawanna, V. Y. Kulkarni, R. A. Rane, P. Mestri, S. Panchal," Risk Rating System of X.509 Certificates," 12th International Multi-Conference on Information Processing-2016 (IMCIP-2016), Bangalore, India,pp.152-161,2016.

[34] S.Anooshiravan, M.U.Janjua, N.Porter, P. Hallin, H.Li, X.Su, K.Yiu, A.P.Penta, V.D.Bakalov, B.M.Nitta," Advising Clients about Certificate Authority Trust," patent application at Politics & Government Week, February 25, 2016

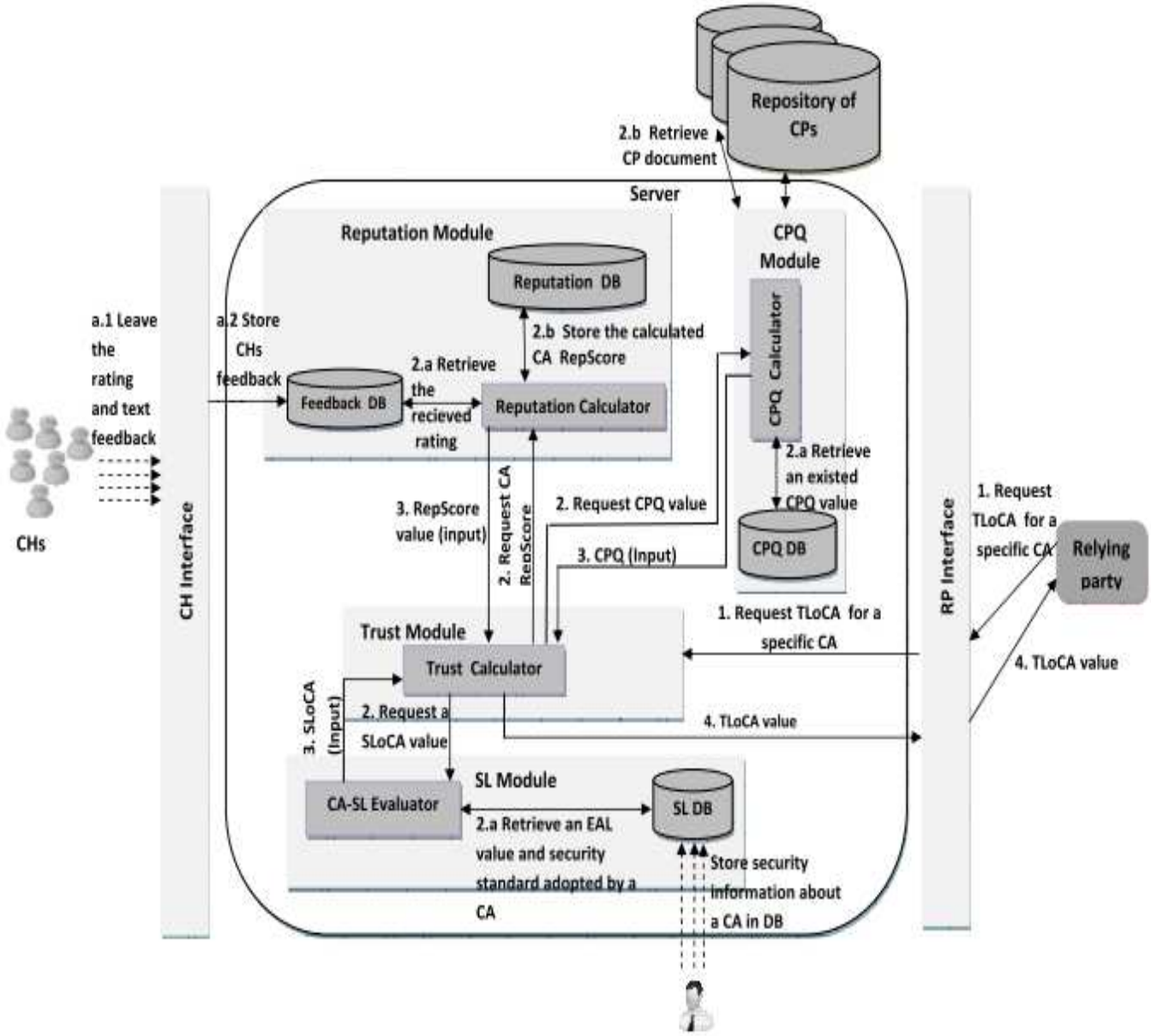

Figure 2. Proposed trust framework

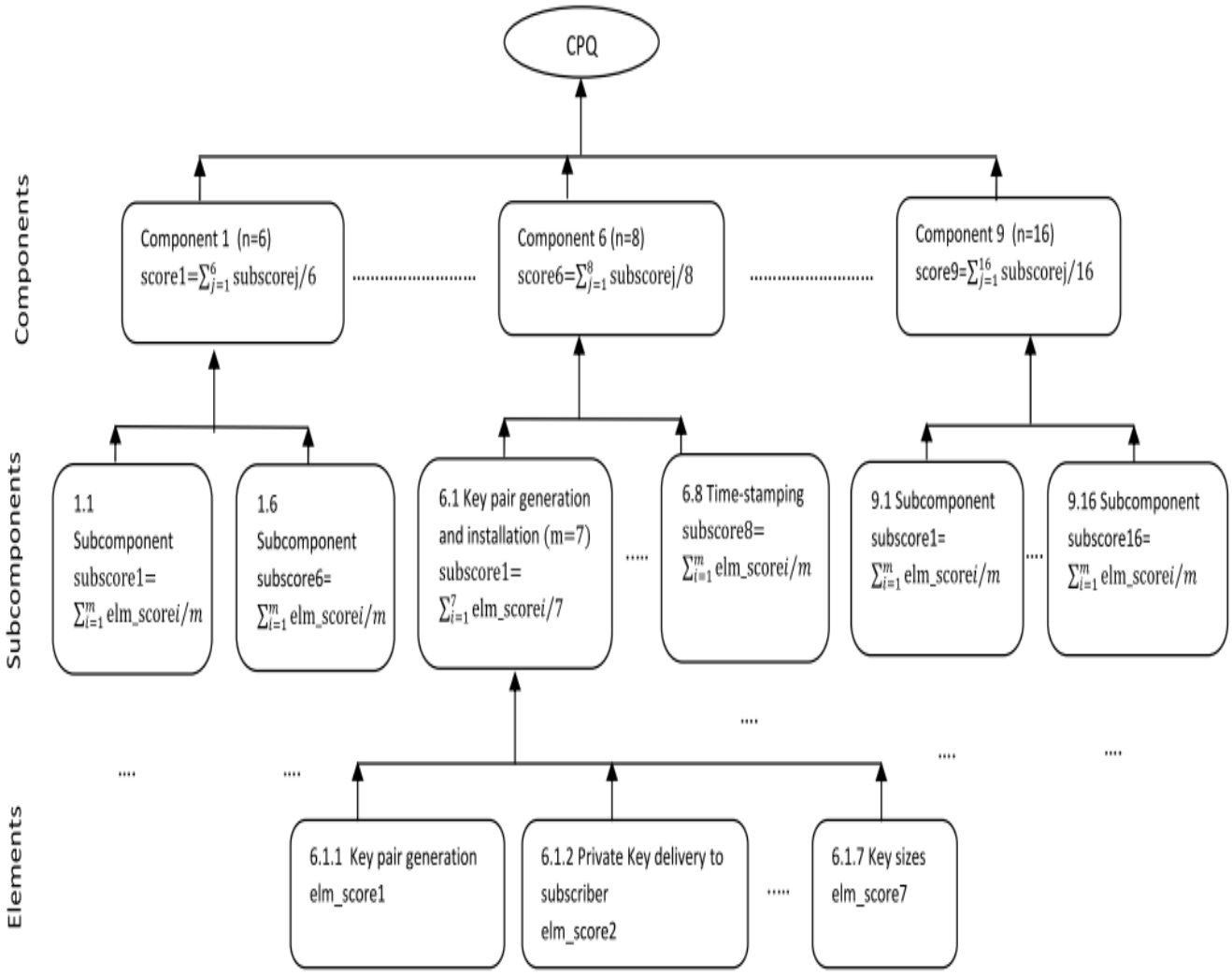

Figure 3. Tree structure representing a certificate policy