Scientific Research Publishing

Journal of Information Security, 2020, 11, 241-260
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Public Key Infrastructure: An Enhanced Validation Framework

Paul Danquah[1], Henoch Kwabena-Adade[2]

[1]Council for Scientific and Industrial Research-Institute for Scientific and Technological Information (CSIR-INSTI), Accra, Ghana
[2]Accra Institute of Technology (AIT), Accra, Ghana
Email: pauldanquah@yahoo.com, henochx@gmail.com

How to cite this paper: Danquah, P. and Kwabena-Adade, H. (2020) Public Key Infrastructure: An Enhanced Validation Framework. *Journal of Information Security*, **11**, 241-260.
https://doi.org/10.4236/jis.2020.114016

Received: July 18, 2020
Accepted: September 22, 2020
Published: September 25, 2020

Abstract

Public Key Infrastructure (PKI) is a comprehensive information security framework for providing secure information and communication over the internet. Its need and use has grown over the years and continually grows. This research work examines the current PKI framework's validation process as operated by vendors and subscribers to identify the drawbacks and propose enhanced approaches to its validation mechanism. Using an approach of reviewing secondary data, critical weaknesses of integrity, proof of trust and single point-of-failure were identified with the current PKI framework. This study therefore advances proposed solutions to address the identified weaknesses by specifically introducing multiple Certificate Authorities, storage, visibility and searchability of subscriber information in public repository. A comprehensive detail of its implementation is proposed to address the identified weaknesses of uncertain integrity, trust for certificate authorities and prevent a single point of failure. Furthermore, the proposed enhancements are validated with the protection motivation theory and a framework for empirically testing the enhancements is suggested. Further research would be required to factor in multi-factor authentication without compromising performance.

Keywords

Security, Public Key Infrastructure, PKI Validation, Cyber Security

1. Introduction

A public key infrastructure (PKI) is a framework that is used in creating and managing digital certificates and public key encryption [1]. The essence is to assist the safe transfer of electronic information for a variety of web activities such as private mailing, e-commerce and internet based banking. The framework

specifically makes it possible to create, use, store, manage, distribute, and annul digital certificates and manage public-key encryption. PKI is a foundation for establishing trusted communication on a network; the field has developed as the footing to deliver secure data communication and internet security. "Identification and authentication, data integrity, confidentiality, and technical non-repudiation combined are elements that provide a secure, non-breakable environment for any type of electronic transaction" [2].

PKI has become the platform or the infrastructure upon which symmetric and asymmetric encryption scheme services are provided to everyone that subscribes to it, it is therefore required in situations where more rigorous proof is essential to check the identity of the parties communicating and to authenticate the information being transferred.

PKI tends to link public keys with various respective entities that have unique identities. These are referred to as subscribers. This linkage is made possible via the process of registration and issuance of certificates by authorized organizations referred to as Certificate Authority (CA). The process of registration where requests for digital certificates are accepted and the requesting entity authenticated is done by organizations is referred to as Registration Authority (RA). In the PKI framework, an entity must have a unique identity within each CA domain; the uniqueness is typically based on information provided by and about that entity. According to [3] PKI plays a critical role in helping a business deliver basic controls such as ensuring confidentiality and integrity in essential business practices.

Despite this well-established infrastructure to assist the secure transfer of electronic information, numerous concerns have been raised about the adequacy of its validation mechanisms and overall security robustness.

A CA may be compromised or may act maliciously [4]; in the case one CA is compromised, and all domains on the specific CA are in danger [5]. Also it advances that the use of a CA introduces a single point of failure, and history has proved that we put too much trust in the CA since they could make mistakes and issue the wrong type of certificates. [5] posits that "only one CA with a certification path to a trusted root CA is needed to be compromised in order to allow the attacker to issue fraudulent certificates". Concerns are also raised about the fact that besides attacks from the outside, a CA or its resellers can also misuse their power to issue a fraudulent certificate for a domain. In suggesting a public key infrastructure for the Internet of Things, it was concluded that a secure enrollment and certificate overhead reduction was essential [6].

The objective of the proposed work is to evaluate current PKI validation methods with the aim of proposing enhanced methods for the PKI validation framework. The scope is focused on the PKI's current validation framework.

The motivation behind this research is to investigate the weaknesses in an attempt to propose solutions to the PKI framework. Browsers have the capability to detect malicious websites that have forged or fake Secure Socket Layer (SSL) certificates, but existing cryptographic solutions do not have the efficient capa-

bility in detecting malicious websites with mistakenly issued or compromised certificate authority (CA), browsers cannot detect such fake certificates because the CA that signs the certificate appears to be in good standing, giving users false impression about the websites being visited.

The research sets out to extend the understanding of the PKI infrastructure, its methods, operations and theory, possible ways it can be enhanced and the weakness inherent in the infrastructure, possible future upgrades and revisions. The essential output and contribution of this research work the proposal of solutions to address the identified weaknesses by specifically introducing multiple certificate authorities, storage, visibility and searchability of subscriber information in public repository.

This paper is organized here forth by an explanation of the research method(s), a review of related literature and a proposal of the enhanced framework for PKI validation based on findings from literature. Furthermore, the enhanced framework is theoretically validated, its functional test framework is proposed and conclusions are drawn.

2. Methodology

This research work deployed a predominantly desk review and descriptive approach. Descriptive research design aids in the provision of solutions to the queries related to a particular research problem and can produce rich data that lead to relevant recommendations in practice. This approach collected a large amount of data for detailed analysis [7], "it is effective to analyze non-quantified topics and issues, the possibility to observe the phenomenon in a completely natural and unchanged natural environment, the opportunity to integrate the qualitative and quantitative methods of data collection". A predominantly secondary source of data is used and qualitatively analyzed to deduce strengths and weaknesses for the current PKI validation methods.

3. Literature Review and Related Work

A vital advantage of public-key cryptography over symmetric key cryptography is that it enables unfamiliar persons or parties to communicate securely without the need for prior introduction between the parties. This is possible because these individuals/strangers are bound to unique public keys which are used to encrypt messages intended for them. Since trust is a major concern, the binding is done by third parties who are trust worthy or trusted by both sender and recipient. In the event that a large user population consisting of several thousands or millions of entities, the utmost useful way to achieve this is to employ a reasonably small number of authorities trusted by perhaps, the entire population [8]. In the event of a change of identity, a private key compromised, or certificate expires, the key-pair binding is no longer valid, and it is rendered invalid. There must be a way to communicate this invalidity to all users. Certificate revocation list (CRL) is used for that purpose. CRLs comprise a list of revoked certificates

[9].

Rastegari, Susilo, and Dakhilalian [10] proposed the Certificateless public key cryptography (CL-PKC) as a means to overcome the problems of PKI and ID-based settings. "In conventional PKI, CAs are assumed to be fully trusted. However, in practice, CAs' absolute responsibility for providing trustworthiness caused major security and privacy issues" [11]. A new PKI architecture was therefore proposed with "certificate transparency based on blockchain called CertLedger, to eliminate the split-world attacks and to provide certificate/revocation transparency". This is yet to be deployed widely for thorough testing.

Infrastructures in general are built on an architecture. PKI is built on client server architecture. The agent being used on the user's local platform must send a request for certification services from the servers. The client agent software is an important component of a complete, fully operational PKI [12].

A fully functional PKI incorporates certification authority, certificate repository, certificate revocation, key backup and recovery, automatic key update, key history management, cross-certification, support for non-repudiation, time stamping and client software. **Figure 1** is a diagrammatic representation of the current PKI validation process.

Public Key Encryption Methods and Algorithms evolved from [14] Rivest, Shamir, and Adleman (RSA) and was premised on Integer-factorization schemes, Diffie-Hellman Key exchange was based on discrete logarithm schemes, Digital Signature Algorithm (DSA) based on Elgamal encryption or Digital signature algorithm, Elliptic curve Diffie-Hellman key exchange (ECDH) based on Elliptic curve schemes and the Elliptic curve digital signature algorithms premised on elliptic curves that can offer stages of security with short length keys. Public key schemes can be used to provide services such as confidentiality, digital certificate, non-repudiation, digital signature, data integrity and key establishment [15]. A number of weaknesses have however been identified for the PKI, an academic research report authored by a team from the school of informatics and computing at Indiana University Bloomington, Software bugs and misinterpretations of industry standards accounts for 42% of incorrectly-issued SSL certificates.

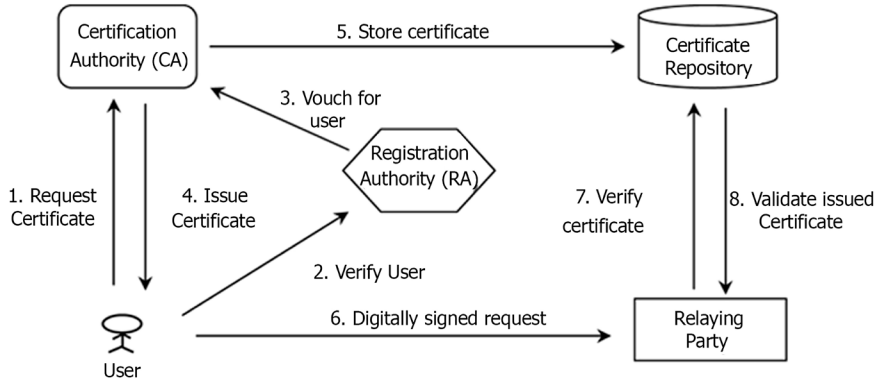

Figure 1. A public key infrastructure. Source: Sinnott, 2011 [13].

The research looked at 379 instances of miss-issued SSL certificates from a total of over 1300 known incidents [16].

3.1. X509 Certificates

A very essential certificate standard is the X.509 standard. The X509 certificates are of two types: namely public key certificate which combines public keys to a subject as stated earlier and attribute certificate that binds attributes such as roles to a subject. There are also however alternatives to the X509 certificates [17].

The term certificate in this context refers to the x509 public key certificate standard which is also referred to as public key certificate. X509 is the certificate format issued by certificate authorities to both CAs and end users alike [8].

Public key Certificates remain the most critical piece of component to the operations of PKI. Certificates to a large extent are public keys which have been signed by trusted CAs and can be distributed publicly like any file for instance word document file. Certificates contain data and have format similar to any type of file with format. Figure 2 is an overview of the certificate structure.

Further Figure 3 is sample generated private and public key using a key management software.

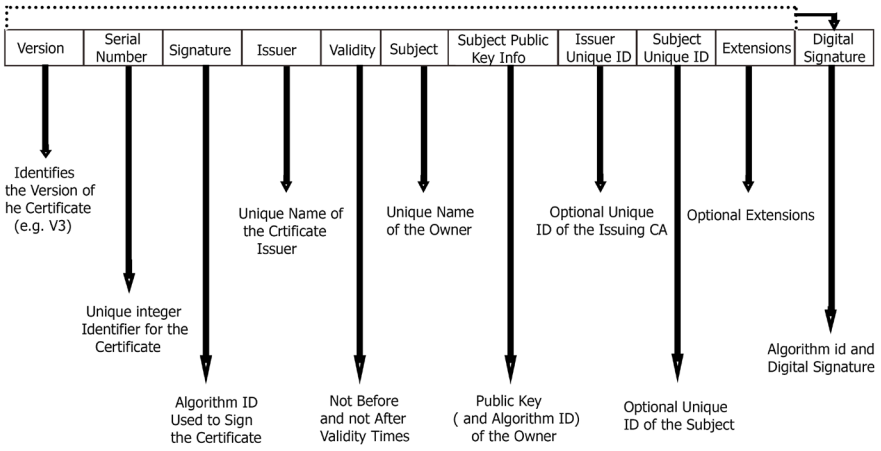

Figure 2. X509 version 3 certificate structure.

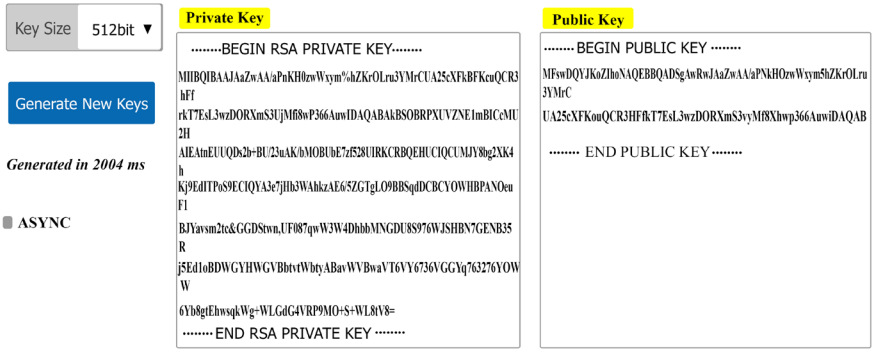

Figure 3. Generated RSA public-private key pair. Source: Researcher Field Work.

For the purposes of illustrating a signed certificate, Figure 4 shows a key that has been signed by the certificate authority hence is now a public key.

3.2. PKI Architecture and Trust Models

PKI architecture is premised on the quantity of CAs involved, their organization, and the association between them [9]. The need for different PKI architectures, also known as trust models by industry players, largely depends on varied needs and processes of business, this implies that, PKI trust models are as a result of the requirements and demands of business. "Direct trust is the most basic trust model, it is therefore required by all other trust models to initialize trust" [12]. This implies that for any kind of architecture or trust model, there must exist some form of direct trust without which no trust can be initialized. This therefore implies that trust must start from somewhere and be propagated to where it is needed. Direct trust is the highest form of trust and it is obtained when users directly acquire the public keys of CAs directly from the CA via out of band means. For example, embedding the public keys of Digicert in Firefox or Microsoft browsers.

For such trust models to be functional, just as users need to trust CAs, CAs in an infrastructure need to trust each other. A basic component of PKI is that public keys, usually structured as signed certificates, must be trusted. The inability to

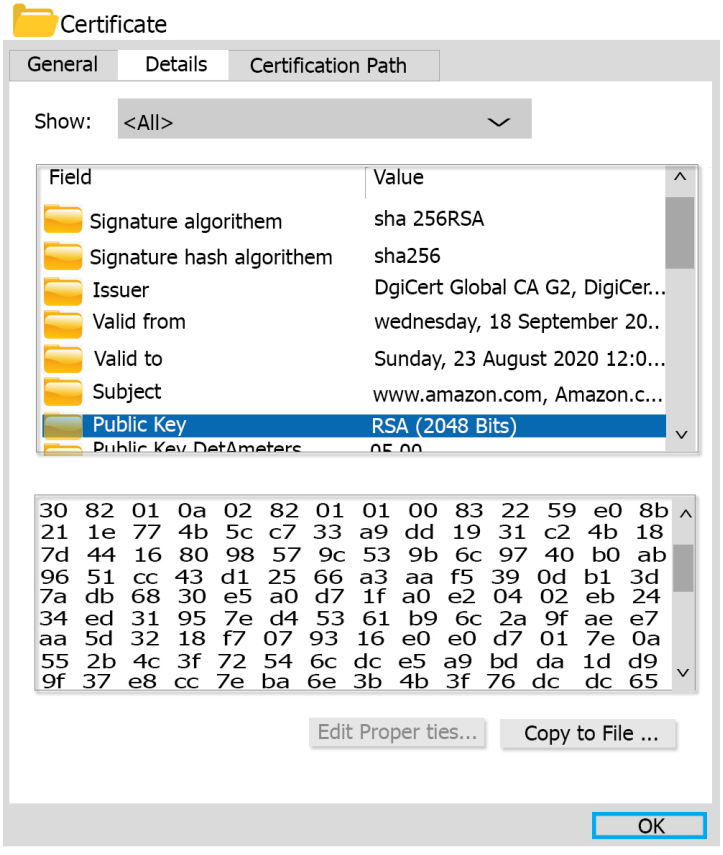

Figure 4. Sample digital certificate issued by DigiCert to Amazon.

ensure the required level of trust causes the entire PKI to negatively experience a grave "weak link in the chain" [18].

The PKI architecture types have no single point of view that exists today especially on the naming conventions used. Different types of PKI architecture have been discussed in many literatures. However, all these types can be grouped into three main categories due to similarities in their operations.

According to [10], "PKI architectures can be implemented in the following ways: Single CA architecture, Enterprise PKI architecture and Hybrid PKI architecture". However, [18], suggest that the general construction of a PKI is denoted as non-hierarchical, hierarchical, or cross-certified.

This research work operationalizes the definition of Choudhury *et al.* with three main PKI trust models.

A single CA Architecture or Single trust model involves only one CA and all users trust this single CA. This CA explains the set of certificates that it can verify and trust.

A PKI with a single CA architecture suffers from scalability issues, single point of failure, difficulty of management and limited scope, etc. These limitations motivated the various models with multiple CAs with different arrangements. In other words, PKI architecture is defined by the number of CAs providing the PKI services, and roles played by the CAs defines their relationship. Users in a single CA model cannot be trusted, by users in another CA since there is no trust between the CAs and they operate independently. This implies that there is no interoperability between users and CAs in single CA models whiles, interoperability remains very important to the growth of business.

Single CA model is capable of addressing the requirements of small organizations, this tends to be however inadequate in situations where the organization's requirement grow with the need to be interoperable and requirements tend to be more complex. This is typically the operations of a single CA to be distributed and arranged between multiple CAs. PKI services are provided by multiple CAs; a tiered construction with subordinate CA relationships in which all users trust a single "root" CA. Its operation requires the root CA to issue certificates to subordinate CAs only, the subordinates can issue certificates to users or CAs in lower levels of the hierarchy. The trust relationship is specified in only one direction, and every certification path begins with the root CA's public key. There must exist direct trust for the root CAs for the system to be trustworthy.

In a tiered or hierarchical PKI, trust in the genuineness of a public key is established via a certification path. If a CA is the entity of a certificate issued by another CA, the certificate is called a cross certificate. In hierarchical model, there are a number of cross certifications. "A list of cross certificates needed to allow a particular user to obtain the public key of another entity, is known as a certification path. In a hierarchical PKI, trust in the authenticity of a public key is established via a certification path" [12]. The most common PKI architecture deployed by organizations is the Hierarchical [9]. This assertion is confirmed by [19], it is explained that a root CA at the topmost delivers all the information

and the in-between CAs in the tiered structure only trust information provided by the root. The root CA also trusts in-between CAs that are in their level in the tiered structure.

This arrangement allows a high level of control at all levels of the hierarchical tree. Thus, hierarchical models allow tight control over certificate-based activities.

3.3. Certification Path

Certificate path is a predetermined arrangement of certificates with the predefined features that in all related certificates with the exception of the last one operate on the premise of the subject being the issuer of the subsequent certificate. Certificate path validations are performed by algorithms known as certification validation algorithms. These algorithms verify that a given certificate path is valid under a given public key infrastructure (PKI).

When a relying party such as Alice in Figure 5, is presented with any certificate she does not already or explicitly trusts, Alice will use path validation to make an informed trust decision.

In Figure 5, Alice trusts the public key of Diana, however, for the trust to be established, the following path validation is used. The chain commences with the certificate that is self-signed by the root CA. The subsequent has the root CA certifying the public key of CA2. The third certificate then has CA2 certifying the public key of Diana.

3.4. Cases of Breached PKI Security

A challenge associated with the CA's hierarchical model of trust relationships is that in the event that the root CA's private key is compromised, the entire tiered structure of the CAs and end entity certificates collapses. Essentially, if a CA's private key is ever compromised, the breach could be leveraged to falsify messages in-between entities, in the event this is reliant on a certification path that includes that of the CA's and possibly many paths are routed through the CA, it

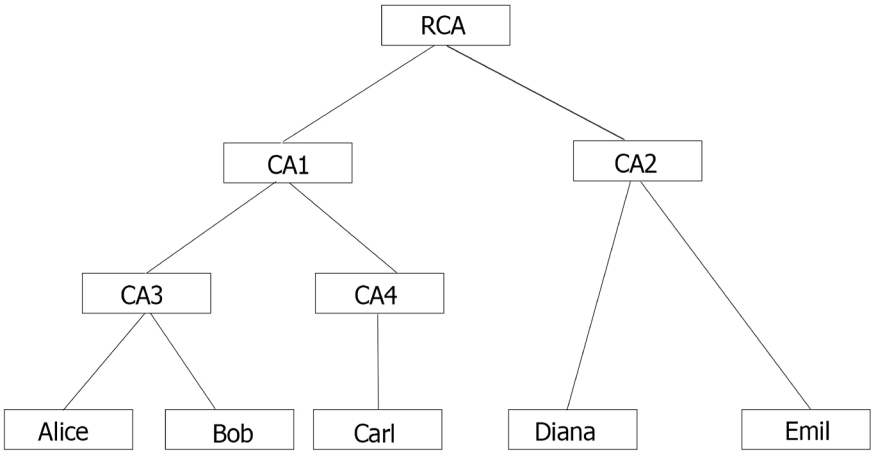

Figure 5. A simple hierarchical PKI. Source: [12].

invariably provides an available target for security breach attacks. Should a key be compromised, it can no longer be trusted and should be replaced [20].

In 2011 two important root Certificate Authority, Comodo and DigiNotar, were compromised. "The attacker who penetrated the Dutch CA DigiNotar had complete control of all eight of the company's certificate-issuing servers during the operation and he may also have issued some rogue certificates that have not yet been identified" [21].

The case of compromise of the certificate vendor called Comodo, the culprit said he has successfully breached another CA, in addition to two more Comodo partners [22]. Security is considered to be a chain; it is therefore considered to be only as strong as its weakest link. This involves people, technology and processes, not everything is dependent on cryptography, [23], an employee from StartCom was able to get a domain certificate for "mozilla.com" from CertStar, a Registration Authority of Comodo. There was no validation at all at the Registration Authority in the certificate request [16].

The certification model for X.509 concentrates validation power into the hands of a few professionals, who are not necessarily well-intentioned, or at least not always competent. [24]. Failure of a CA signing key is catastrophic; keys could be compromised without anyone's knowledge. The possible compromise of a CA's private key signifies a single point-of-failure0 has the potential to create far reaching consequences [25].

Just like any system, there is no such thing as 100% security proof. PKI suffers from various attacks. Equally, there have been different, and variants proposed solutions from industry players to remedy such security breaches and reduce the attack surface of PKI.

In summary, it is important to understand some fundamental principles that ensure inter-domains certificate validation possible. There are multiple CAs in the Hierarchy model as stated earlier, there is a root CA and subordinate CA and the end entities. For cross certification purposes, it is required that CAs will issue certificates to other CAs, whereas some CAs issue certificates to end entities or users, this implies that, there are two primary types of public key Certificates: user certificates and CA certificates.

3.5. Public Key Infrastructure Strengths

Public Key Infrastructure is well noted for some strengths; it is considered relatively more secure than passwords. Malevolent users or attackers must obtain both the private key and the matching passphrase to fake as a legitimate user, PKI in this context provides stronger identity checking through secret private keys [26]. PKI is greatly scalable because there is no limit to the number of users who can be supported using PKI [27]. The permission of the trust delegation in PKI prevents man-in-the-middle (MitM) attacks, this is a result of its possibility without knowledge of the key pair. This is possible once a user with a legitimate certificate from a recognized and trusted certificate authority is able to authenticate himself to a server the very first time. The connection to the server is possi-

ble without having previously been registered with the system. This makes it possible for the PKI to enable a trustworthy setting by validating and ensuring the integrity of data and users. The keys within PKI established systems can be used for one-way encryption functions where only the designated owner of the key can decrypt data. [28]. PKI also has the benefit of private keys which are difficult to crack together with the corresponding public key. "As such, it features cryptographic protection that passwords lack: passwords do not necessarily have a verifiable, computable relationship with anything" [29]. PKI enables added service offerings such as banking, law, health care, e-commerce and intelligence, through the use of digital signatures and digital certificates. It detects tampering and allows for non-repudiation [30]. The seamless, ease and non-interactive use of PKI is key strength and driver for PKI's overall acceptance.

3.6. Public Key Infrastructure Weaknesses

Certificate Authorities have had several slips where they issued certificates without adhering to rules. CAs have issued SSL certificates that have been used to perform man-in-the-middle (MitM) attacks and intercept HTTPS traffic have been used for malware operations or CAs issued certificates without following standard procedures because of human errors, accident, or to cut costs and increase profits [16]. As long as certificate issuance remains a business, the motivation to increase profit and cut down cost is eminent. Thus, according to the report, CAs issue certificate without following standards. Such standards include subscriber validations which can be costly especially for extended validations (EV). "Extended validation is costly. CAs need to employ different information sources, undergo additional CA/Browser forum procedural steps and pay for additional third-party audits to issue EV certificates. Companies require additional employee training, internal audit systems and the like which all translate into cost" [31]. It therefore makes economic sense to cut cost and increase profit. The main PKI weakness is that, a certificate can be signed by any certificate authority for an individual or machine. There is also the situation where certificate authorities are made coerced to certificates for entities they have no business vouching for [32].

The certification model for X.509 essences endorsement power into the hands of a few specialists, who are not necessarily always competent or well-intentioned. When a CA is not well-intentioned, it could issue rogue certificates, and will not adhere to standards and best practices. PKIs are heavily dependent on the integrity CAs and RAs, these CAs and RAs aren't always necessarily functional at the perfect professional level of conscientiousness and scrutiny [33].

This incident emphasizes the possibility of CAs to issue certificate to domains without validation. It also implies that CAs can issue certificate without the permission or authorization of domain owners.

Additionally, a security lapse of Public Key Infrastructures today is the lack of multi-factor authentication on many of the top frameworks [33] (Venafi education, 2019). CA can use keys fraudulently, negligently, erroneously or mistakenly

without detection. The keys can be lost or stolen, that is, keys can be misused or lost. CA and RA are considered as trusted parties in PKI, likewise in cryptographic literature, this perception of trust however cannot be evidenced or confirmed with certainty.

Failure of a CA signing key is catastrophic; keys could be compromised without anyone's knowledge. The management and revocation of certificates requires a highly complicated structure. Complexity is a weakness of PKI Visibility.

The essentially deduced Public Key Infrastructure weaknesses identified are therefore namely uncertain integrity, absence of multi-factor authentication, insufficient proof of trust and the potential of a single point of failure

4. Enhanced Framework for PKI Validation

The goal of the proposed solution is to enhance PKI validation by enhancing integrity, trust of CAs and avoid a single point of failure. Fundamental to the process is the need for a subscriber's information to be searchable and retrievable in the public repository before any certificate authority can sign a certificate. Further to this, if reliance on the private key is distributed or shared among separate CAs, which means more than a single private key is required to generate a valid certificate and the would-be owner of the certificate is required to authorize specific CA in signing public keys, it will no longer be an attractive option to target a single key as it is the case currently.

If certificate signing becomes transparent and highly controlled and monitored, it will reduce the rate of compromise of private keys for unauthorized usage and consequently reduce revocation currency.

The proposed solution will not require any changes in the generation of private keys by the CAs and the process of signing of certificates. However, it involves additions and enhancement to the existing PKI and relies on the concepts of Certificate Transparency logs and Certificate pinning as stated previously and introduces new registration mechanisms for validation enhancement similar to Domain Name System registration and services.

CAs will be required to operate in similar manner as domain name registrars, where name registration request is cross checked with other names registrations authorities from a database to avoid duplicate and forgery of name registration.

In this regard, certain CAs operations like signing and registration processes will not be conducted in isolation, they shall be required to operate collaboratively. That is even though a domain registrar is autonomous in its operation, it is required of it to verify the existence of a domain name or otherwise, from a common database accessible to all. Controlled certificate signing process and monitoring of certificates issuance, means that certificate signing, and issuance is highly regulated.

Figure 6 is a diagrammatic representation of the process involved in subscription,

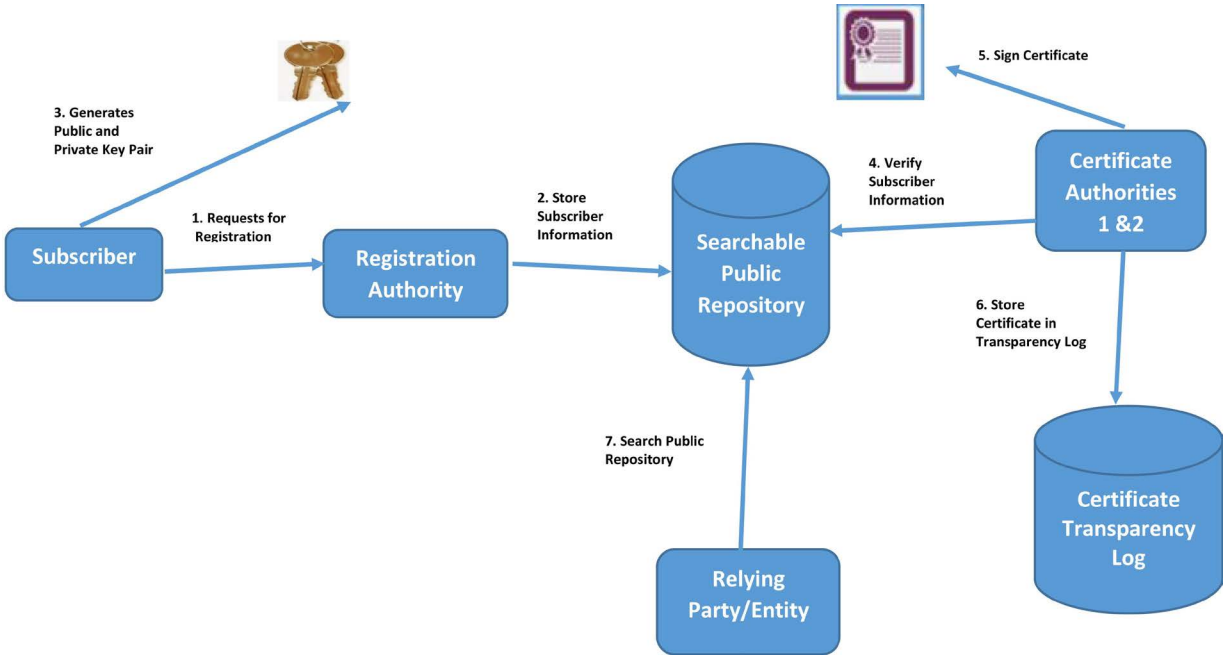

Figure 6. Enhanced validation process. Source: Researcher Field Work.

validation, signing and accessibility of the certificates.

4.1. Enhanced Validation Procedure

1) Requests for Registration: The stage of the process involves the subscriber applying to a registration authority to obtain signed certificates.

2) Store Subscriber Information: The registration authority registers the subscriber and stores the subscriber details in the public repository to make subscriber information publicly searchable and visible.

3) Generates Public and Private Key Pair: The subscriber uses a key management system to generate keys to be made available for signing.

4) Verify Subscriber Information: The certificate authority validates authenticity of subscription/application and then signs the keys.

5) Sign Certificate: Certificate authority signs the keys to certify subscription.

6) Store Certificate in Transparency Log: The certificate authority proceeds to store the certificate in transparency log to make certificate publicly available.

7) Search Public Repository: The certificates are made available and searchable in the public repository for relying entities to access certificates for use.

4.2. Discussion on Enhanced PKI Validation

Comparatively, the process described in Figure 1 conspicuously omits the storage of subscriber information for public accessibility, mandatory verification of subscriber information to validate authenticity and the collaboration of two certificate authorities to sign and certify the subscriptions as compared to Figure 6. The dependencies proposed in Table 1 provide a premise for the respectively outlined stages.

Table 1. Details of PKI validation process stages, purpose, novelty and dependency.

No.	Process/Stage	Actor/Entity	Purpose	Novelty	Dependency
1	Requests for Registration from Registration Authority	Subscriber	To obtain signed certificates	No	No Dependency
2	Store Subscriber Information	Registration Authority	To make subscriber information publicly searchable and visible	Yes	Dependent on Successfully Registered Subscriber
3	Generates Public and Private Key Pair	Subscriber	To make keys available for signing	No	No Dependency
4	Verify Subscriber Information	Certificate Authority	To validate authenticity of subscription/subscriber	No	Dependent on Successfully Registered Subscriber and information stored in Public Repository
5	Two CAs Sign Certificate	Certificate Authority	To certify subscription	Yes	Dependent on Generated Certificates
6	Store Certificate in Transparency Log	Certificate Authority	To make certificate publicly available	No	Dependent on Signed Certificates
7	Search Public Repository	Relying Entity	Access Certificates for use	No	No Dependency

The proposed solution eliminates potential mistakes, errors, forgery and impersonation during enrolment. Multiple validation processes by different CAs with different approaches to information gathering and validation methods will not capture the same mistakes and errors, rather it will assist in capturing any inconsistencies.

Detection of unlawful or wrong entry in the registration record can be easily detected since those records are publicly available and searchable. It is also possible to write simple scripts to automatically monitor the online repository for specific domain entries to immediately detect any anomaly or unauthorized entries.

It provides certificate governance and reduces autonomous operation since CAs cannot operate in isolation or issue out certificate without the cooperation of the online repository, the subscriber and the issuing CAs. This implies that certificate issuance is not centrally controlled or monopolized, thus PKI operations are distributed

The proposed solution ensures accuracy of subscriber records as records can be monitored continuously with very little efforts to immediately detect any suspicious entries for specific domains. Because the online repository is searchable and read only, only authorized entities can modify the entries which ensures that accurate records are maintained.

CAs will police each other, this will ensure high level of compliance and adherence to best practices and standards without compromising to save cost or resources. It will ensure quality in the overall validation process whiles enforcing the procedures.

As the validation records are made public, the subscriber can later detect errors or mistakes for immediate corrections. It also implies that once the online data is correct, it can guarantee the accuracy of the certificate to be issued and

the validation process of the relying parties.

The included novel component of storing subscriber information for public accessibility impacts positively on both trust of registration authority and integrity of the process and ultimately the certificate authority, the component of mandatory verification of subscriber information to validate authenticity also impacts positively on trust and integrity of the certificate authority and the process. The component of collaboration of two certificate authorities to sign and certify the keys in the PKI validation process prevents a possible single point of failure. This is illustrated in Table 2.

At the point of registration, the subscriber decides and indicates the preferred certificate authorities and essentially has this information stored and publicly visible. The usage of two certificate authorities subsequently prevents the possible single point of failure in the event that one certificate authority is compromised. Browsers would require re-configuration to ensure that they check for two certificate authorities in signed certificates.

4.3. Improved Trust

Trust is the safe confidence in the competence of an individual or entity to act securely, dependably, reliably and timely within a specified context.

To prove the existence of trust means to prove the reliability of the trust. The proposed framework requires both participation of the subscriber and the CA. The CA alone cannot operate in isolation. An attempt to sign a certificate for a domain without the approval of the domain owners or pre-registration by the would-be subscriber will fail since the owner approval is required before signing can be executed. Thus, because signing of a certificate in the proposed system requires permission and authorization from domain owner, it is easy to prove or verify the trustworthiness of the infrastructure. Thus, the subscriber is not just trusting the CA to only do what is expected of it, but it can be proved that the CA cannot secretly execute harmful unauthorized task on its own. The reliability and dependability of the proposed solution is improved.

Table 2. Illustration of PKI enhancements.

No.	Process/Stage	Purpose	Enhancement
1	Requests for Registration from Registration Authority	To obtain signed certificates	None
2	Store Subscriber Information	To make subscriber information publicly searchable and visible	Trust of registration authority and integrity of the process
3	Generates Public and Private Key Pair	To make keys available for signing	None
4	Verify Subscriber Information	To validate authenticity of subscription/subscriber	None
5	Two CAs Sign Certificate	To certify keys of subscription/subscriber	Prevents a possible single point of failure
6	Store Certificate in Transparency Log	To make certificate publicly available	None
7	Search Public Repository	Access Certificates for use	None

4.4. Enhanced Integrity

Integrity is the assurance of data being complete, consistent and free from any form of corruption. In this context, it is the subscriber who requires assurance that information provided, stored and recorded cannot be altered.

Only domain owners could initiate and authorize certificate signing requests, only authorized certificate authorities could sign certificates and only authorized administrators could have access to the signing private keys protected with multi factor authentication. Thus, all stake holders need to be compromised to undermine the integrity of the proposed framework. One would notice if the secure key for multifactor authentication went missing, so a private signing key being protected by the missing secure key could be revoked immediately before it is compromised by an attacker.

4.5. Optimal Performance

Predominantly, browsers are required to consider multiple certification paths pending the discovery a valid one for a given certificate. "Constructing and evaluating all possible paths is an expensive process performed for every new certificate a browser encounter" [34].

This implies that, for a certificate to be verified, a browser would have to obtain a series of certificates referred to as a certification path each one having signed the next certificate in the sequence, connecting the signing CA's root which is the trust anchor to the server's certificate called the leaf. Longer certification paths take much time and require more resources to process.

In the proposed solution, the registration record also serves as trusted anchor validation database. Every issuing or intermediate CA in the registration record would have been vetted, validated and approved by the trusted anchors, therefore, there is no need to construct longer certification path chains from the leaf to the anchor by browsers. This reduces the certification path length. The issuing CAs certificates are the only required certificates in the certification path. Therefore, the time it takes to construct, validate and process certificates for verification is expected to minimize, consequently minimizing resource utilization by relying parties.

5. Theoretical Validation

The earlier background provided explains the fact that PKI comprises various systems and procedures needed to generate, allocate, use, store and revoke digital certificates and accomplish public-key encryption management. The primary objective is to protect electronic transfer of information for various network activities. These range from internet banking to e-commerce and email. Fundamentally, its need is essential authentication methods available require a rigorous proof to ascertain identity of the parties involved in the communication and to validate the information being transferred.

The protection motivation theory which was first published in 1975 empha-

sized on fear appeals and attitude change, this was further revised in 1983 to address cognitive and physiological processes in fear-based attitude change [35]. Theoretically, the Protection Motivation Theory (PMT) proposes that people protect themselves based on four factors:

1) Perceived Severity: The perceived severity of a threatening event

2) Perceived Vulnerability: The perceived probability of the occurrence, or vulnerability

3) Fear Response Efficacy: The efficacy of the recommended preventive behavior

4) Perceived Self-Efficacy: The belief that one can successfully perform the recommended action

These proposals are consistent with the enhancements suggested for the PKI infrastructure validation framework. The two enhancements namely; Store Subscriber Information and Two CAs Sign Certificate tend to make subscriber information publicly searchable, visible, trust of registration authority, ensures integrity of the process and certifies keys of subscription/subscriber as well prevents possible single point of failure respectively.

Relative to the PMT, storing the subscriber information for public visibility envisages the potential of a subscriber not being authentic hence inherently considered as vulnerability, the perceived vulnerability in this context spirals into a potentially major impact upon compromise hence the perceived potential severity in any form of threatening event. Further to this, the enhancement where two CAs sign certificates prevent possible single point of failure, thereby enhancing the efficacy of the recommended preventive behavior with the belief that the recommended action can successfully be performed within the framework.

Technically, the two proposed enhancements would complement the PMT and enhance overall PKI implementations in the event subscribers' information becomes publicly visible and searchable as well design browsers to validate the two CAs during the PKI validation process. It is therefore essential to note that the PKI enhancement further binds public keys with respective identities of entities via a practice of registration and issuance of certificates at and by two certificate authorities.

6. Functional Test of Framework

The functional test seeks to establish that the proposed solution operates in conformance with the set objectives and expected possible outcomes based on specific inputs. The system either validates or invalidates certificate.

A testing browser or relying party may reject certificate signed by one CA, thus when a browser receives a certificate, it validates the certificate by ensuring that there are two CAs in the issuer field. If a certificate received by the browser is signed by two CAs, but those CAs have not been registered with the subscriber in the online registry repository, the browser may reject that certificate as invalid even though the certificate is signed by two CAs. Thus, the test is expected to

accept a certificate as valid only when the required number of CAs who are authorized or registered with that subscriber has duly signed the certificate.

The procedures to test the proposed solution require modifications to the certificate extension fields of X.509 V3 Certificate and the browser requirements baseline.

Certificate Extension Fields Modifications: Certificate capabilities can be enhanced via the use of extensions to modify the issuer field. For this test, this field must be modified to contain the distinguished names information of the two CAs which signed the certificate instead of one distinguished name.

Further to this, an extension field must be defined in the certificate to provide the link to the online registration repository database. This extension must provide the location to the publicly searchable registration records of the RA.

The browser baseline requirements configuration must be done to read the online repository records and the issuer field distinguished names and compare both data. The validity of the certificate depends on the outcome of the comparison.

The certificate is only accepted, and connection established if the data read in the issuer distinguished name field matches exactly the data fetched from the online registration repository. Thus, a match in both records means that, the certificate was requested by the right subscriber, with right information and was issued by the right CAs.

The certificate is however rejected, and connection refused if the data read in the issuer distinguished name field mismatches the data fetched from the online registration repository. That is, the certificate is valid if a match is found and rejected if a match is not found.

The central registration record is updated by CAs whereas the current private key generation by the CA is maintained

There are two expected outputs of the test framework. These are namely:

1) Display of a warning page, if validation fails.

2) Display of the intended webpage, if validation is successful.

For the purpose of this functional test framework, it assumed that documentation for validation is accurate and readily available, there is reliable internet connectivity, subscriber is responsive, there is no misconfiguration, no latency on internet connection, length of time to issue standard certificate with e-mail and CNAME based Validation is 8 minutes' maximum and expected length of time to issue extended validation certificate is 18 days' maximum.

7. Conclusion

PKI usage continues to grow at a fast pace; with the internet of things being the main driver for this growth, future computing devices will continue in the trend of getting faster, more powerful, more reliable and more portable. The trend of ever rising speed of broadband Internet connections will in the long future continue to get faster. The advancement in technology especially the rising speeds of

internet connections means that internet connection speed is no longer limitations of online systems as it used to be in time past. Mobile devices are capable of full desktop computing tasks and high speed broadband internet access. Processing PKI validation and verification in this proposed framework would provide the needed benefits without compromising performance and efficiency as the computing devices and the internet platform are both capable of such computing tasks. Having advanced the proposed solutions to address the identified weaknesses by specifically introducing multiple Certificate Authorities, storage, visibility and search ability of subscriber information in public repository, it is recommended that further research is carried out in multi-factor authentication without compromising overall PKI performance.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Lynch (2017) Hashed Out. https://www.thesslstore.com/blog/wide-world-pki

[2] Homeland Security, DISA Provides Public Key Infrastructure Security for the Mobile Environment. https://www.hstoday.us/subject-matter-areas/infrastructure-security/disa-provides-public-key-infrastructure-security-for-the-mobile-environment

[3] Ricks, M., Simakov, S. and Rabourn, S. (2014) Securing Public Key Infrastructure (PKI). Microsoft IT Information Security and Risk Management, 126.

[4] Doowon, K., Kwon, B.J. and Dumitras, T. (2017) Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI.

[5] Soltani, S.Z. (2013) Improving PKI Solution Analysis in Case of CA Compromisation.

[6] Höglund, J., Lindemer, S., Furuhed, M. and Raza, S. (2020) PKI4IoT: Towards Public Key Infrastructure for the Internet of Things. *Computers & Security*, **89**, Article ID: 101658. https://doi.org/10.1016/j.cose.2019.101658

[7] Dudovskiy, J. (2018) The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance. Sage Publications, New York.

[8] Adams, C. and Lloyd, S. (2003) Understanding Public-Key Infrastructure. Macmillan Technical Pub., Indianapolis.

[9] Choudhury, S., Bhatnagar, K. and Haque, W. (2002) Public Key Infrastructure Implementation and Design. M&T Books, New York.

[10] Rastegari, P., Susilo, W. and Dakhilalian, M. (2019) Certificateless Designated Verifier Signature Revisited: Achieving a Concrete Scheme in the Standard Model. *International Journal of Information Security*, **18**, 619-635. https://doi.org/10.1007/s10207-019-00430-5

[11] Kubilay, M.Y., Kiraz, M.S. and Mantar, H.A. (2019) CertLedger: A New PKI Model with Certificate Transparency Based on Blockchain. *Computers and Security*, **85**, 333-352. https://doi.org/10.1016/j.cose.2019.05.013

[12] Karatsiolis, E., Wiesmaier, A. and Buchmann, J. (2013) Introduction to Public Key Infrastructures. Springer-Verlag, New York.

[13] Sinnott, R. (2011) Public Key Infrastructure. https://www.researchgate.net/figure/A-public-key-infrastructure_fig1_220566584

[14] Sheets, D. (2019) Trusted Computing. https://www.militaryaerospace.com/trusted-computing/article/14035441/trusted-computing-algorithms-asymmetric

[15] Kessler, G.C. (2019) An Overview of Cryptography. https://www.garykessler.net/library/crypto.html#skc

[16] Serrano, N., Hadan, H., *et al.* (2019) A Complete Study of P.K.I. (PKI's Known Incidents). https://doi.org/10.2139/ssrn.3425554

[17] Park, C. (2017) A Secure and Efficient ECQV Implicit Certificate Issuance Protocol for the Internet of Things Applications. *IEEE Sensors Journal*, **17**, 2215-2223. https://doi.org/10.1109/JSEN.2016.2625821

[18] Johner, H., Fujiwara, S., Yeung, A.S., Stephanou, A. and Whitmore, J. (2000) Deploying a Public Key Infrastructure. Redbooks.

[19] Meghdadshamsaei (2017) Trust Model Implementation with PKI. http://shamsaei.com/author/meghdadshamsaei

[20] Stock, A. (2005) Guide to Building Secure Web Applications and Web Services. https://www.links.org/files/CertificateAuthorityTransparencyandAuditability.pdf

[21] Fisher, D. (2012) Final Report on DigiNotar Hack Shows Total Compromise of CA Servers. https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170

[22] McMillan, B.R. (2011) Comodo Hacker Claims Another Certificate Authority. https://www.pcworld.com/article/223760/article.html

[23] Ellison, C. and Schneier, B. (2000) Ten Risks of PKI. *Computer Security Journal*, **16**, 1-8.

[24] Willeke, J. (2019) LdapWiki. https://ldapwiki.com/wiki/Public%20Key%20Infrastructure%20Weaknesses

[25] Bargav, J., Li, H. and Evans, D. (2017) Decentralized Certificate Authorities. https://oblivc.org/dca

[26] SSH (2019) Advantages and Disadvantages of Public-Key Authentication. https://www.ssh.com/manuals/server-zos-product/55/ch06s02s02.html

[27] Oracle (2002) The Public Key Infrastructure Approach to Security. https://docs.oracle.com/cd/B10501_01/network.920/a96582/pki.htm

[28] Cooper, M.B. (2018) PKI EXPLAINED. https://cybersecurity.isaca.org/articles-details?articleId=pki-explained-why-it-is-necessary-and-relevant-now-more-than-ever

[29] Fortinet (2019) How to Apply PKI Client Authentication. https://help.fortinet.com/fweb/591/Content/FortiWeb/fortiweb-admin/apply_pki_client_auth.htm

[30] Natalie, R. (2019). https://greengarageblog.org/8-pros-and-cons-of-asymmetric-encryption https://www.ssl.com/article/browsers-and-certificate-validation

[31] Callan, T. (2019) Why CAs Charge More for Extended Validation SSL. https://sectigo.com/blog/why-cas-charge-more-for-extended-validation-ssl

[32] SSH Communications (2019) PKI-Public Key Infrastructure. https://www.ssh.com/pki

[33] Venafi (2019) How Does PKI Work.
https://www.venafi.com/education-center/pki/how-does-pki-work

[34] Naziridis (2019) Browsers and Certificate Validation.
https://www.ssl.com/article/browsers-and-certificate-validation

[35] Rogers, R.W. (1983) Cognitive and Physiological Processes in Fear-Based Attitude Change: A Revised Theory of Protection Motivation. In: Cacioppo, J. and Petty, R., Eds., *Social Psychophysiology*: *A Source Book*, Guilford Press, New York, 153-176.