Journal of Information Security, 2015, 6, 31-37
Published Online January 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.61004

Public Key Infrastructure: A Survey

Aysha Albarqi[1], Ethar Alzaid[1], Fatimah Al Ghamdi[1], Somaya Asiri[1], Jayaprakash Kar[2]

[1]Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, KSA
[2]Department of Information Systems, Information Security Research Group, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, KSA
Email: jayaprakashkar@yahoo.com

Received 25 September 2014; revised 5 November 2014; accepted 10 December 2014

Abstract

As security is essential in communications through electronic networks, development of structures providing high levels of security is needed. Public Key Infrastructure (PKI) is a way of providing security measures by implementing the means of key pairs among users. In this paper, an overview of the public key infrastructure is discussed that includes various components and operation, some well known PKIs and their comparisons. Also we discuss current implementations, risk and challenges of PKIs.

Keywords

Impersonating Attack, Ephemeral Key, Compromise Attack, Certificate Repository

1. Introduction

The demand for securing communications is increasing dramatically day by day. Along with this demand, more techniques have been proposed to achieve the maximum security. The most commonly used technique is the encryption with two kinds of cryptography. First one is called private key or symmetric cryptography; it can be applied really fast but the key is hard to be managed since there is just one key each user. Despite this issue, it still plays a role in the most encryption systems. Other kind of cryptography is proposed to overcome this issue under the name of public key or asymmetric cryptography where each user is provided with a pair of keys: public and private keys. Since the public key is not a secret, then the key management problem was solved but equivalent problem was raised which is the authentication or name management problem. Public key infrastructure (PKI) was developed to solve this problem and support the public key cryptography. Authentication is the process of using all PKIs. We have introduced several PKIs with different architectures and processes and briefly discussed a comprehensive survey of these PKIs.

How to cite this paper: Albarqi, A., Alzaid, E., Al Ghamdi, F., Asiri, S. and Kar, J. (2015) Public Key Infrastructure: A Survey. *Journal of Information Security*, **6**, 31-37. http://dx.doi.org/10.4236/jis.2015.61004

2. PKI Overview

PKI is an abbreviation of the Public Key Infrastructure, it was developed to support the public key (asymmetric) cryptography. In this type of cryptography, the message is going to be encrypted by the sender using the public key of the receiver and then this receiver, presumably, is the only one who can decrypt this message using the corresponding private key. This direction in cryptography was introduced since 1976 [1], to solve the key management problem, using a directory called Public File in which entries are name, number and public key. The sender looks the recipient up in the Public File by his name to find his public key. By this scenario, the sender does not have the complete confidence that the key truly belong to desired recipient. Kohnfelder [2] proposed a solution by certificate or digitally sign each entry in the "Public File", so the certificates could be distributed through a network securely.

In the 1980's, International Telecommunication Union (ITU) decided to build a larger directory to cover all people and devices all over the world, so the result was a standard called X.500 [3], defining all characteristics of that directory. Another standard called X.509 was proposed for authentication purposes, nobody could change any entry in a directory except if he has permission. A X.509 standard defines the certificate format; it binds the identity of the key holder to the holders public key. All theses evolutions in public key cryptography have lead to build a public key infrastructure (PKI) in which the digital certificates present the heart of it. For more trust authority, Certification Authority (CA) was introduced [4], which is a trusted party responsible for verify and sign the certificates. Therefore, PKI has helped the sender to retrieve the public key of desired recipient with the confidence that this key is really recipient's public key. Recently, various models of PKI have developed with different schemes; the paper will present some of these models and discuss the most popular ones. Taxonomy of the survey is shown in **Figure 1**.

3. PKI's Component and Operation

The basic common operations in all PKIs are certification and validation. The fundamental function in all PKIs is certification where it is the binds the value of public key to an entity in an authentic way. The other operation is validation, it is the process of verifying the validity of the certifications (still valid or not). A complete public key infrastructure is composed of several components which are: registration authority (RA), certificate authority (CA), security policy, PKI-enabled applications, distribution system, and certificate repository [5] [6]. The components of the PKI are shown in **Figure 2** and are described as.

- **Certificate Authority (CA)**: It's also called Certificate Issuer, which is used to issues the certificates and the revocation lists. A certificate is a data structure composed of both the public key value and the identified information that belong to the holder of the corresponding private key [4]. Each public key certificate is issued to an individual and each certificate has a digital signature of the issuing CA. The certificates have a lifetime of one or two years. The certificate might be revoked for several reasons such as loss of private key, compromise key or the lifetime of the certificate is terminated, etc. If any one of these situations happened; the entity who issued the certificate should be requested to invalidated (revoke) the certificate of public key. There are multiple revocation mechanisms to revoke the certificate and to allow the user to be able to check the validity of the certificate (the certificate still valid or has been revoked). All revocations mechanism needs to be timely and efficient. One of the revocation mechanism is CRL (Certificate Revocation List) which is a list contains certificate the have been revoked and signed digitally by the entity who had issued those certificates previously [5] [7] [8].
- **Registration Authority (RA)**: is used to submit all the requests to the CA and authenticates all the users identities and registers the end user's information before certification. The services given by RA can be accessible through two ways:

  1) Logging the administrator through the browser to the system.
  2) Calling the web services interface through the application system.

  RA has only one super administrator which can access all the functions provided by RA where this super administrator can add more administrators if needed. Every administrator who wants managing the system must use its own smart card to prevent unauthenticated people from making any operations to the registration authority (RA) [6] [7].
- **Distribution System and Certificate Repository**: are used to provide storing mechanism, they store the certifications and CRL information [6]. The complexity of PKI can be hidden from client system by adding one more component which is Validation Authority (VA) which responds to the client requests for certificates

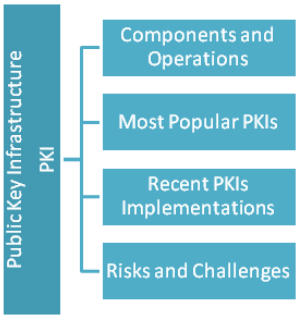

Figure 1. Taxonomy of the survey.

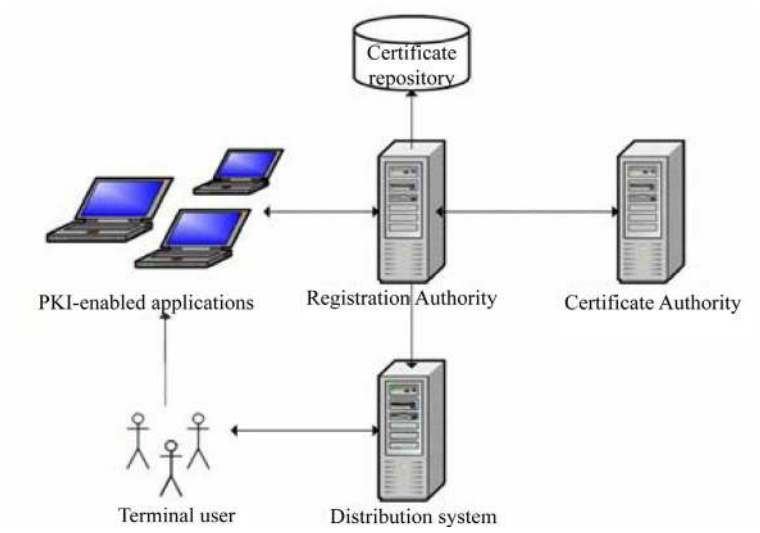

Figure 2. PKI's components.

revocation status and doing the accessibility valuation of certificates on the behalf of the client system [7] [9].

The protocol operations of the PKI and actors are shown in **Figure 3** where the protocol operations indicated by numbers. The protocol operations of the PKI in the figure above are:

- **Certificate generation and Key**: Registration Authority establishes the key holder identity and passes his/her information with the public key for certification to the CA. Then the CA or the owner of key can generate the key pair, where the most important point is the safe transportation of the private key to the holder of key. A typical lifetime is one year for a certificate after which a new certificate is issued.
- **Revocation list generation**: Making a list of all non-expired or revoked certificates where the CA signed these lists then sent them either to the VA or sent them immediately to the relying parties where there is no need for online status provider to doing the validation. The revocation lists generation interval is four hours.
- **Signature generation**: The holder of key making signs for a message including his/her public key certificate with the signature data. The frequency was chosen of the signed messages is 300 messages per day for every active user where this number has been chosen for the purpose of the forthcoming calculations.
- **Certificate validation**: The status of revocation of the signer's certificate must be checked by the relying party where it can be done either by checking the revocation list that most recently available or by querying the VA. The frequency of the operations that belongs to the validation is the aggregate frequency of the received messages—among all users—by the relying party [7] [10].

4. Well Known PKIs

Taking trust as a classification scheme, PKIs can be distributed into several trust models. Some PKIs relies on the trust of a single authority "CA" and some other relies on the trust of users between each other. In this section, two of the most common models are to be discussed.

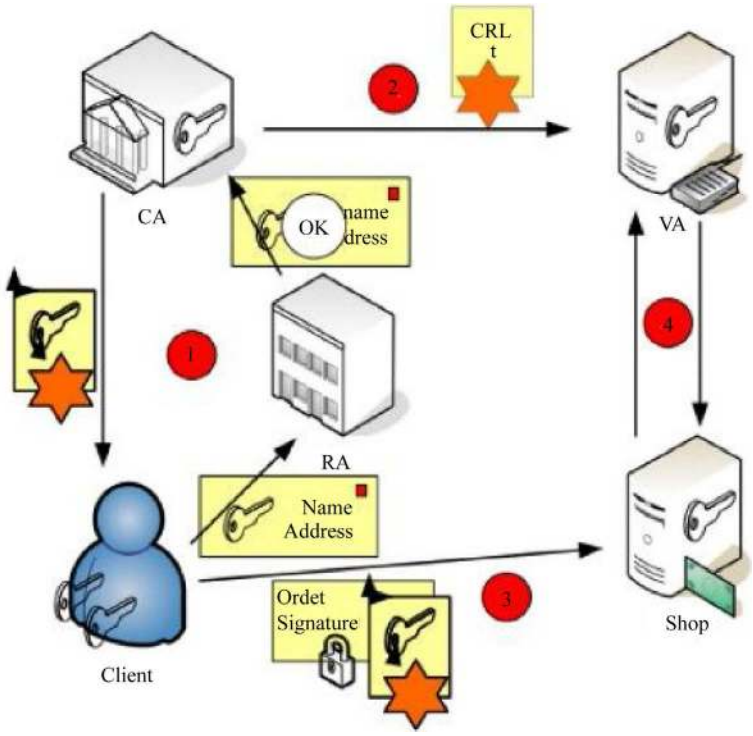

Figure 3. Protocol operations and actors of the PKI.

4.1. Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is common Public Key Infrastructures and one of the most popular ones being used. Phil Zimmermann is the designer of this infrastructure in 1991, it uses a concept called "Web-of-Trust" where users generates their own key pairs and publish them to be signed by other PGP users to build up a trusting relationship between the generators and the signers.

Most PKIs uses some authority to define the level of trust among users; so an advantage of using PGP arises. The independence of a governor over keys due to trust constructed between users makes using PGP easier. Each user has a public-ring where received keys are being stored and assigned levels of trust depending on a decision of the end user, while other infrastructures use a central authority to perform validation and verification. A user can set policies and rules on the level of trust; for example: a key will not be accepted unless it was signed by three other trusted keys. On the other hand, a user can accept a non-signed key on a user's own risk [11].

Regarding revocation of keys, it is also the authority of the key holder to revoke the key using a signed message for revocation and then posted to a public server. When a user sees such message, he/she has to remove the key from the public-ring storage. Revocation messages have to be signed by the key holder, so it is quite impossible to send a fake revocation message unless the key has been compromised. If a revocation message has been produced from a compromised key; it is a good improvement for security of the overall system, as a consequence of considering such message as a warning for the other users so they would not trust that key [12]. Even though such a warning message might be sent to the other users to avoid communication with the key, the holder cannot guarantee that every other user has received and read the revocation message. To avoid such problem, the key holder can add an option field to the certificate including an address to a personal web site where other key holders can check the holder's key status. Many different places PGP users can use to check the status of the keys but they would not be sure if the information is being updated or not.

4.2. Internet X.509 Public Key Infrastructure (PKIX)

Since 1995, working group to support PKIs has been established under the name of PKIX "Internet X.509 Public Key Infrastructure". As we have mentioned in the overview section, X.509 carries the authentication role in X.500 directory services and both of them are proposed by "International Telecommunications Union

Telecommunications Standardization Sector" [12]. PKIX model is based on a Certifying Authority (CA) system that issues public key certificates (PKCs) in order to distribute public keys among the end entities that hold private keys [12].

To start using the PKI, user first needs to register by sending a request for a PKC to a CA. This request contains some required information like the user's name and some attributes put in his PKC. A CA before issue certificate, it will verify the provided information either by itself or by registration authority (RA) then it signed with private key of CA. A PKC contains some information like CA's name, end entity's name with its public key, a certificate serial number, a validity period and other associated information. In order to validate a certificate, the relying party calls the public key of CA and verifies the certificates signature, checks that date is within the validity period, and may also perform other online checks [12].

In this model, there is a hierarchic chain of CAs to validate the certificate; starts by the self-signed root certificate until reaches the end entity certificate. Once the chain has been verified by the relying party, signature on the end-entity's certificate is trusted to be proper, and then go to validate other information such as public key, validity periods to fully trust the certificate by contacting the CA [12].

PKIX comes with few protocols that aim to perform on line status checking on the certificates; one most widely used is Online Certificate Status Protocol (OCSP). And for more specification, PKIX proposes periodically published certificate revocation lists (CRLs) to check revocation status of a certificate.

4.3. Comparison between PGP and PKIX

On the following table some of the differences have been pointed out to compare between the two PKIs.

5. Current Implementations of PKI

During the last decades, many improvements have been introduced to the traditional public key infrastructure to make it suitable for different platforms such as mobile environment, smart grid applications, etc. In this section we will briefly present some of the recent models.

- **WPKI**: Wired infrastructure usually deals with devices with high computational power with large memory size and robust source of power. On the other hand, wireless devices have more technical limitations such as less powerful CPU with lower memory size and limited source of power (battery), which made the need for another infrastructure that complies with the wireless limitations and capabilities. Wireless Public Key Infrastructure (WPKI) [13] provides wireless devices (mobile phones for an instance) with the same security level as a wired PKI.
- **LPKI**: Lightweight Public Key Infrastructure (LPKI) [14] is proposed to support the mobile environments. It applies the features of elliptic curve cryptography and signcryption [15]. LPKI establishes many enhancements to the conventional PKIX in order to make it cost-effectively and more appropriate for the mobile environment and other resource constrained platforms. In this model, a new unit was introduced called Validation Authority (VA) to eliminate all computational costs of required validations. LPKI has a compact compatibility with PKIX infrastructure since the certificates in both of them are based on the format of the X.509v3 certificates.

6. Risk and Challenges of PKI

Overall security of electronic transactions is almost impossible although it is designed to secure PKI transactions. Cases of security breach are still occurring due to human error or slackness. This section will take a look at some of the risks related to PKI.

6.1. Private Key Protection

The core foundation of PKI is the key pair public and private keys. Particularly, customer's private keys are the major components of the PKI. If the private key of the client was stolen, And Can be used to digitally sign the private key by fraud steers as if the same client. If the private key of the CA is stolen, fraud steer can use this key for generate a lot of digital fraud.

The most common way to protect the private key stored on a device is using passwords. However, the situation is not safe when simple passwords are used they can be guessed easily, especially if it is as simple as

passwords “abc123” or chosen “12345678”. Another way to protect your private key using “smart cards” [15], it is used one time and then disposed of. Each card has a private key unique password. This method is more secure, as the private key does not leave the card and the card itself never perform all the functions depending on the user and the key to these functions, such as encryption, signing, verification of the electronic message. But should buy the card from a trusted source, so that this source is not known for mechanical security used.

6.2. Non-Repudiation in PKI

Although PKI provides a level of trust between individuals, as mentioned in the previous section, the attacker can access the private key of someone, and then he or she can generate messages signed by the key holder. In this case, it would be almost impossible to prove that key holder did not send the message. PKI is created to cover such problem.

The user can perform necessary to ensure that the end of the infrastructure is safe, but cannot be confident if the other users (or even CA) are doing their part. The question here is: Is CA doing a comprehensive verification of the identity of all customers. CA aims to ensure that all certificates issued by the old keys are not being used again. Such questions increase doubts about the security and reliability of the PKI [16].

6.3. Open PKI Liability Risks

PKI has many applications, which reduces the administrative burden and improve the experience for the end user, for example; Reducing the number of passwords makes it easier for the user to remember .Of the biggest challenges is how to PKI allows the applications especially the best-of-kind applications required by enterprise customers generally. Two approaches are used by PKI vendors:

- **Closed PKI**: is a kind of proprietary software issued a limited number of digital certificates, therefore can control the applications and users who need communicate securely. But the closed PKI systems need a lot of training, software, hardware, and maintenance
- **Open PKI**: “Applications interface seamlessly with certificates issued under an open PKI, the roots of which are already embedded. Open PKI systems allow enterprises to become their own CA, while taking advantage of the PKI vendor’s service and support.

In the field of e-commerce, cheating and theft are inevitable. Although the PKI is established to prevent these threats from happening, but they might occur if all parties involved in the PKI are open to a reasonable extent. Risk management is fundamental in both types of PKI; closed and open PKI. And the responsibility control is easy because they are limited in scope and which is supposed to be performed by the CA. Positive aspect of the closed PKI is that it can predict the potential risks, the owner can either imbibe the losses himself, or he can pass it off to his customer. Certificate Authorities bear the a larger role in protecting an open PKI model because board certified are referenced to verify the identity of individuals or certain institutions, and issued this body digital certificates to prove that the individual or organization known by this authority, depends on this body in ensuring the rights of dealers via the Internet as they provided documents proving get deal between two parties specific. So it should CA to verify that the vendors they deal with their trusted [17].

Responsibility is not taken only by the CA. CA customers should take the necessary measures to save their own data. The most important reviewing contracts and certificates from CA to ensure lack of erroneous data. Customer holds a great deal of risk if used fakes certificates are no longer supported by the CA. Despite the lack of an ideal solution for the protection of electronic data transfer. PKI is a good solution at the present time. It combines the functionalities of public/private key, digital certificates, and hashing algorithms to reach a high level Security and confidentiality of data and non-repudiation. There are those criticize the way in which the ratification of the certificates in the PKI [18]. These terms refer to the weakness of reliability in the verification process carried out by the CA in proof of identity certificate applicant. As there are those who question the extent of confidentiality and security of the devices that match the signatures or those used In keeping private keys. However, many believe that the Internet has opened up many opportunities require secure infrastructure, such as those available by the technique remained. Despite the constraints and uncertainties, but it can be solved by the creation of the necessary laws to ensure the safety of electronic trading and trust in him.

7. Conclusion

As security has become an essential need for any system to guarantee safe communication among users, the

need for a technique to secure those channels became a demand. Public Key Infrastructure offers many ways to secure communications depending on the type or level of security needed. The paper has gone through the main components of a PKI and what operations they are assigned to. There are many infrastructures in the area and the paper discussed two of the main PKIs: PGP and X.509 besides a brief overview of the two new PKIs: WPKI and LPKI where they match the needs of the current devices and technologies. As in anything related to using a technique, PKI has its own risks when being used and those risks were discussed in the paper. In the end, the authors hope they have made a contribution by going through the main aspects of an important security application.

Acknowledgements

We would like to thank to our supervisor Dr. Jayaprakash Kar for his valuable suggestions and comments that helped improving this works. This support is greatly appreciated.

References

[1] Diffie, W. and Hellman, M.E. (1976) New Directions in Cryptography. *IEEE Transactions on Information Theory*, **IT-22**, 644-654.

[2] Kohnfelder, L.M. (1978) Towards a Practical Public Key Cryptosystem. MIT S.B. Thesis, Massachusetts Institute of Technology, Cambridge.

[3] ITU-T (1993) The Directory—Overview of Concepts, Models and Service. X.500 Series of Recommendations, International Telecommunications Union, Geneva.

[4] Ford, W. (1998) Public Key Infrastructure Interoperation. *IEEE Aerospace Conference*, 21-28 March 1998, Snowmass at Aspen, Vol. 4, 329-333.

[5] Chokhani, S. (1994) Toward a National Public Key Infrastructure. *IEEE Communications Magazine*, **32**, 70-74.

[6] Wang, K.F. and Zhang, Z.H. (2010) Design and Implementation of a Safe Public Key Infrastructure. *International Conference on Future Information Technology and Management Engineering* (*FITME*), Changzhou, 9-10 October 2010, 298-301.

[7] Fongen, A. (2010) Optimization of a Public Key Infrastructure. *Military Communications Conference* (*MILCOM*), Baltimore, 7-10 November 2011, 1440-1447.

[8] Wing, P. and O'higgins, B. (1999) Using Public Key Infrastructures for Security and Risk Management. *IEEE Communications Magazine*, **37**, 71-73.

[9] Polk, W., Hastings, N. and Malpani, A. (2003) Public Key Infrastructures That Satisfy Security Goals. *IEEE Internet Computing*, **7**, 60-67.

[10] Dankers, J., Garefalakis, T., Schaffelhofer, R. and Wright, T. (2002) Public Key Infrastructure in Mobile Systems. *IEEE Electronics and Communications Engineering Journal*, **14**, 180-190.

[11] Slagell, A., Bonilla, R. and Yurcik, W. (2006) A Survey of PKI Components and Scalability Issues. 25*th IEEE Performance*, *Computing*, *and Communications Conference*, Phoenix, 10-12 April 2006, 10 p.

[12] Vacca, J. (2013) Public Key Infrastructure. In: *Cyber Security and IT Infrastructure Protection*, Steven Elliot, Waltham, 75-107.

[13] Balachandra, M., Krishna, P. and Shashank, S. (2012) Wireless Public Key Infrastructure for Mobile Phones. *International Journal of Network Security and Its Applications* (*IJNSA*), **4**, 111-118.

[14] Toorani, M. and Beheshti, A. (2008) LPKI—A Lightweight Public Key Infrastructure for the Mobile Environments. 11*th IEEE International Conference on Communication Systems*, Guangzhou, 19-21 November 2008, 162-166.

[15] Kar, J. (2014) A Novel Construction of Certificateless Signcryption Scheme for Smart Card. In: *Case Studies in Secure Computing Achievements and Trends*, CRC Press, Taylor and Francis, New York, Chapter-22, 437-456.

[16] Kar, J. (2014) Provably Secure Online/Off-Line Identity-Based Signature Scheme for Wireless Sensor Network. *International Journal of Network Security*, **16**, 26-36.

[17] Kar, J. (2013) ID-Based Deniable Authentication Protocol Based on Diffie-Hellman Problem on Elliptic Curve. *International Journal of Network Security*, **15**, 347-354.

[18] Kar, J. (2014) Authenticated Multiple-Key Establishment Protocol for Wireless Sensor Networks. In: *Case Studies in Secure Computing Achievements and Trends*, CRC Press, Taylor and Francis, New York, Chapter-04, 67-88.

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.