ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 7, July 2013

Public-Key Infrastructure (PKI)

Anju Sharma, Neeraj Goyat, Vinod Saroha

***Abstract* — This paper presents a survey on Public-Key Infrastructure (PKI). This discussion is centered on overview of public-key infrastructure, its key elements, PKI management functions, protocols, digital certificate format and its applications. Public-key infrastructure (PKI) as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography. Public-key infrastructure based on digital certificates and certificate authorties in order to securely implement public key cryptography.**

The principle objectives of developing a PKI is to enable secure, conventional, and efficient acquistion of public keys. A PKI enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

***Index Terms*—PKI, certificate authority, digital certificate, PGP, SSL**

I. INTRODUCTION

Public-key cryptography is a cryptographic technique that enables users to securely communicate on an insecure public network, and reliably verify the identity of a user with the help of digital certificates.

A public-key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates which are used to verify that a particular public keys, securely stores these certificates in a central repositary, and revokes them if required.

Security Services supported by PKI:

- **Authentication** - Ability to verify the identity of an entity
- **Confidentiality** - Protection of information from unauthorized disclosure
- **Data Integrity** - Protection of information from undetected modification
- **Non-repudiation** - Prevention of an entity from denying previous actions
- **Key estalishment**

Manuscript received June, 2013.

***Anju Sharma**, M.tech(network security), B.P.S Mahila Vishwavidhalaya Khanpur Kalan, Sonepat, India,9467772834*

*.**Neeraj Goyat**, M.tech(network security), B.P.S Mahila Vishwavidhalaya Khanpur Kalan, Sonepat, India,9034676338*

***Vinod Saroha**, Asst. Professor (CSE & IT dept.) , B.P.S Mahila Vishwavidhalaya Khanpur Kalan, Sonepat, India , 9416427656*

II. X.509 DIGITAL CERTIFICATE

A digital certificate is a set of data that binds an identity to a particular piece of data. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority. These user certificates are assumes to be created by some trusted certificate authority (CA) and placed in the directory by the CA or by the user.

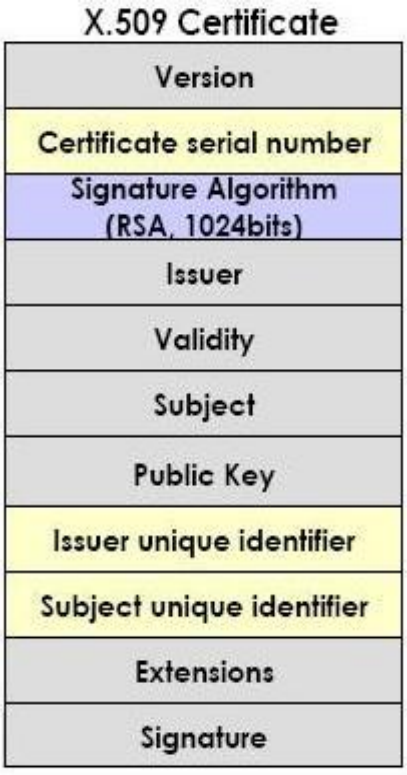

Fig. 1. X.509 certificate

X.509 certificate includes the following elements:

1.Version: - Differentiate among successive versions of certificate format, the default is version 1. If the issuer unique identifier and the subject unique identifier is present, the value must be version 2. If one or more extensions are present, the version must be version 3.

2. *Serial number:* - An integer value, unique within the issuing CA, that is unambiguously associated with each certificate.

3. *Signature algorithm identifier*: - The algorithm used to sign the certificate together with the associated parameters.

4. *Issuer name*: - X.509 name of the CA that created and signed this certificate.

5. *Period of validity:* - Consist of 2 dates: the first and last on which the certificate is valid.
6. *Subject name*: - The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the user who holds the corresponding private key.
7. *Subject's public key information*: - The public key of the user plus the identifier of the algorithm for which this key is to be used, together with any associated parameters.
8. *Issuer unique identifier:* - An optional bit string used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.
9. *Subject unique identifier:* - An optional bit string used to identify uniquely the subject in the event the X.500 name has been reused for different entities.
10. *Extensions*: - A set of one or more extension fields.
11. *Signature*: - Covers all the other field of the certificate; it contains the hash code of the other fields, encrypted with the CA's private key. This field includes the signature algorithm identifier.

The unique identifier fields were added in version 2 to handle the possible reuse of subject and issuer names over time.

III. PUBLIC-KEY INFRASTRUCTURE(PKI)

A PKI allows you to bind public keys with a personthat allows you to trust the certificate. A public-key infrastructure(PKI) is a set of hardware, software, people, policies, and procedure needed to create, manage, distribute, use, store, and revoke digital certificates.

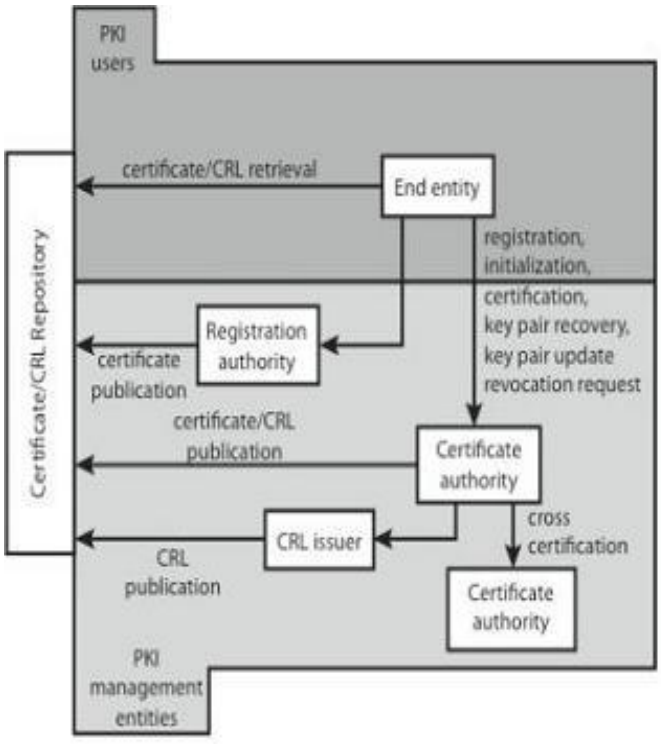

Fig. 2 PKIX Architectural Model

Fig. 2 shows the interrelationship among the key elements of the PKIX model.These elements are

- **End entity:** A generic term used to denote end users, devices (e.g., servers, routers); or any other entity that can be identified in the subject field of a public key certificate. End entities typically consume and/or support PKI related services.
- **Certificate authority (CA):** The issuer of certificates and (usually) certificate revocation lists(CRLs). It may also support a varietyof administrative functions, although these are often delegated to one or more Registration Authoroties.

Some Requirements of certificate authority (CA)

- A physically secure operating environment
- Tamper resistant modules for cryptographic processing (particularly for high-level keys)
- The ability to generate cryptographic keys (a pseudorandom number generator?)
- The ability to check both written and digital signatures
- The ability to sign certificates
- Software to support various certificate formats
- The ability to transport keys securely (perhaps smartcards?)
- A clearly defined security policy
- Auditable procedures for producing certificates
- The ability to maintain certificate revocation lists
- The ability to cover potential financial liabilities.

- **Registration authority (RA):** An optional component that can assume a number of administrative functions from the CA. The RA is often associated with the End Entity registration process, but can assis in a number of other areas as well.
- **CRL issuer:** An optional component that a CA can delegate to publish CRLs.
- **Repository:** A generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by End Entities.

IV. PKIX MANAGEMENT FUNCTIONS

Public Key Infrastructure X.509 (PKIX) identifies a number of management functions that potentially need to be supported by management protocols. These are indicated in Fig. 2 and include the following:

- **Registration:** This is theprocess whereby a user first makes itself known to a CA (directly, or through an RA) , prior to that CA issuing a certificate or certificates for that user. Registration begins the process of enrolling in a PKI. Registration usually involves some offline or online procedure for mutual authentication. Typically, the end entity is issued one or more shared secret keys used for subsequently authentication.
- **Initialization:** Before a client system can operate securely, it is necessary to install key materials that have the appropriate relationshipwith keys stored elsewherein the infrastructure. For example, the client needs to be securely initialized with the public key and other assured information of the trusted CA(s),to be used in validating certificate paths.

- **Certification:** This is the process in which a CA issues a certificate for a user's client system and/or posts that certificate in a repository.
- **Key pair recovery:** Key pairs can be used to support digital signature creation and verification, encryption and decryption, or both. When a key pair is used for encryption/decryption, it is important to provide a mechanism to recover the necessary decryption keys when normal access to the keying materials is no longer possible, otherwise it will not be possible to recover the encrypted data. Loss of access to the decryption key can result from forgotten passwords/PINs, corrupted disk drivers, damage to hardware tokens, and so on. Key pair recovery allows end entities to restore teir encryption/decryption key pair from an authorized key backup facility(typically, the CA that issued the End Entity's certificate).
- **Key pair update:** All key pairs need to be updated regularly (i.e., replaced with a new key pair) and new certificates issued. Update is required when the certificate lifetime expires and as a result of certificate revocation
- **Revocation request:** An authorized person advises a CA of an abnormal situation requiring certificate revocation. Reasons for revocation include private key compromise, change in affiliation, and name change.
- **Cross certification:** Two CAs exchange information used in establishing a cross-certificate. A cross-certificate is a certificate issued by one CA to another CA that contains a CA signature key used for issuing certificates.

V. PKIX MANAGEMENT PROTOCOLS

The PKIX working group has defines two alternative management protocols between PKIX entites that support the management functions:

- RFC 2510 defines the certificate management protocols (CMP).Within CMP, each of the management functions is explictly identfied by specific protocol exchanges. CMP is designedto be a flexible protocol able to accommodate a variety of technical, operational, and business models.
- RFC 2797 defines certificate management messages over CMS (CMC), where CMS refers to RFC 2630, cryptographics messages syntax. CMC is built on earlier work and is intended to leverage existing implementations.

VI. PKI CERTIFICATION METHODS

There are three approaches to getting this trust:

- Certificate authorities : The primary role of the CA is to digitally sign and publish the public key bound to a given user. This is done using the CA's own private key, so that trust in the user key relies on one's trust in the validity of the CA's key. When the CA is a third-party seprate from the user and the system, then it is called Registration Authority(RA), which may or may not be seprate from the CA. The term trusted third party (TTP) may also be used for certificate authority (CA).
- **Web of trust :** An alternative approach to the problem of public authentication of public-key information is the web of trust scheme, which uses self-signed certificates and third party attestations of those certificates. Examples of implementations this is PGP (Preety good privacy)

- **Simple public-key infrastructure:** Another alternative which does not deal with public authentication of public-key information is the simple public-key infrastructure (SPKI) that grew to overcome the complexities of X.509 and PGP's web of trust.PKI does not associate users with persons, since the key is what is trusted, rather than the person. SPKI does not use any notion of trust, as the verifier is also the issuer. This is called an "authorization loop" in SPKI, where authorization is integral to its design.

VII. APPLICATIONS

A PKI is a means to an end, providing the security framework by which PKI-enabled applications can be confidently deployed to achieve the end benefits.
PKIs of one type or another, and from any of several vendors, have many uses, including providing public keys and bindings to user identities which are used for:

- Encyption and/or sender authentication of e-mail messages (e.g, using OpenPGP or S/MIME).
- Encryption and/or authentication of documents(e.g., the XML Signature or XML Encryption standards if documents are encoded as XML.
- Auhentication of users to applications(e.g. smart card log on, client auhentication with SSL.
- Bootstrapping secure communication protocols, such as Internet key exchange (IKE) and SSL.
- Mobile signatures are electronic signatures that are created using a mobile device and rely on signature or certification services in a location independent telecommunication enviornment.

Client-side applications of PKI fit into three main categories:

- **Authentication** applies to any application that needs to know with assurance the identity of the user and that the user is actually the one who is present.PKI provides a more secure alternative to this whereby identity is proven by possession of a private key instead of password. A password is still usually required to protect the private key, but that password is managed locally by the user instead of shared with the application server (a major improvement in security)
- **Digital signatures** is the possession of the private key that assures that only the owner of the PKI

digital credentials could have executed the signature.

- **Encryption** is standard protection of data in afile with a twist. Anyone can encrypt data intended to be read by a particular user by using their public key for the encryption process. But only the designated user posesses the private key that can decrypt the data, so its privacy is assured by the security of the private key.

VIII. CONCLUSION

A main driver of PKI technology is the world's ever-growing dependence on the Internet and all it has to offer is securing all types of e-business activities. Regrettably, four years into the PKI development process, policy-makers and technology-providers have still failed abysmally to appreciate the privacy risks inherent in PKI.

Public key infrastructure based on digital certificates and certificate authorities remain the favoured method for trying to securely implement public key cryptography. There are many complicated issues that arise when trying to implement PKIs, most ofwhich do not have simple or technical solutions. PKI's will not be adopted on a large scale until some of these problems are addressed satisfactorily – the best hope for this is through the establishment of recognized standards and best practice procedures that encourage interoperability between different CAs and PKIs. There are alternatives to traditional PKIs, but these come with their own problems and are most likely to be favoured in various niche application areas.

IX. REFERENCES

1. Wikipedia
2. www.networkmagazine.com
3. http://www.infosyssec.net/infosyssec/pkibib1.htm
4. Network Security by William Stallings
5. www.google.com
6. http://searchsecurity.techtarget.com/definition/PKI

.