ISSN:0975-9646

A comparison between Public key authority and certification authority for distribution of public key

Gaurav Agarwal , Saurabh Singh
Invertis Institute of Engineering and Technology, Bareilly (India)

Abstract: *The key management of public key defines two aspects first one is the distribution of public key and the second one is the use of public key to distribute secret keys for encryption. In this paper we are presenting the public key authentication framework. The distribution of public key can be done by many ways but in this paper we are presenting the two schemes known as the public key authority without certification authority (PKAw CA) and public key authority with certification authority (CA) or certification authority. In this paper we have compared both the schemes with respect to security, availability and their support and prepare a comparison chart for them.*

Keywords: *Public key, Certificate Authority, Key management, Key Backup, Certification Distribution.*

1. Introduction:

In the direction of public key cryptography it is necessary to know the public key of each and every user in network so that the encryption and decryption can be made easily. In this context there are several scheme proposed in "cryptography and network security by William Stallings" like publically announcement of public key, publically available directory, public key authority and certification authority. The use of public key is also available for the generation of secret key. In this paper we are implementing the concept of public key authority without certification authority (PKAwCA) and certification authority (CA).the main purpose is to present the comparison chart between both the schemes under the consideration of security. The two normal schemes to provide the public key in network are.

Public Announcement

A
B
PU_a
PU_a
PU_a
PU_a
PU_b
PU_b
PU_b
PU_b

Figure 1

Where A and B are the two host in the network and PU $_a$ and PU $_b$ are the corresponding public key for A and B respectively and announced publically.

Public Key Directory:

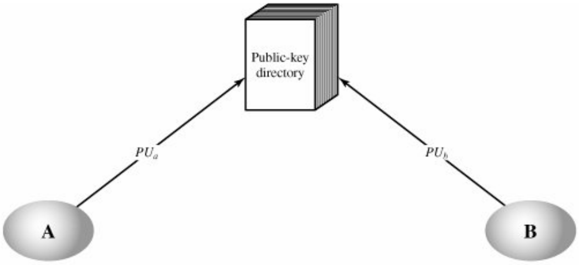

Figure 2

In the public key authority it maintains a greater degree of security in this the public authority maintains a directory with the name and public key for each and every participant. In this each host or system firstly register with its public key to the public key register.

These are the simple distribution of key with in the network.

1.1 Introductions to public key authority:

This is the main concept for stronger security for public key distribution. The whole scenario is illustrated in fig 3 in which the public key directory is responsible to generate the public key for every system.

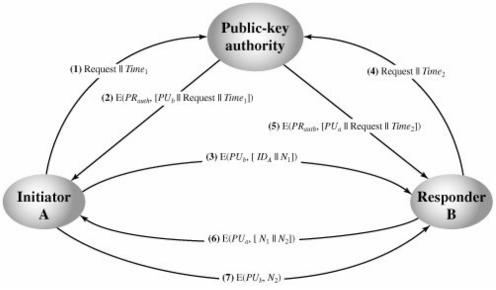
Public-key authority
(1) Request ‖ $Time_1$
(2) E(PR_{auth}, [PU_b ‖ Request ‖ $Time_1$])
(4) Request ‖ $Time_2$
(5) E(PR_{auth}, [PU_a ‖ Request ‖ $Time_2$])
(3) E(PU_b, [ID_A ‖ N_1])
Initiator A
Responder B
(6) E(PU_a, [N_1 ‖ N_2])
(7) E(PU_b, N_2)

Figure 3

The algorithm for public key directory as follows

1- **Request l l Time** $_1$:i.e. Initiator A sends a request with the time step Time 1 for the desired session
2- **E (PR $_{auth}$ [PU $_b$ l l Request l l Time $_1$])**: The original message again sent by the key authority to verify the original request with the public key of responder B.
3- **E (PU$_b$ [Id $_a$ l l N $_1$])**: Now A can store the public key of B and use it to encrypt the message contains the identity of A and a nonce N1: A nonce is used for uniquely identification of every message.
4- **Request l l Time** $_2$: Same process done by as step 1 by the responder B to achieve the public key of A.
5- **E (PR $_{auth}$ [PU $_a$ l l Request l l Time $_2$])** : Process done by the responder B to get the public key of A so that a communication can be established.
6- **E(PU $_a$ [N $_1$ l l N $_2$]):** B sends a message to initiator encrypting with the public key of A and with the nonce N1 as this can assure that the original message was generated by A and it is intended for B.
7- Next and last step A returns the nonce N2, with using the encryption scheme by public key of B to assure that the message was generated by B and intended for A.

This scheme provide a better security aspects for the distribution but there is a lot of use of public key and nonce so there are more possibilities of errors.

1.2 Introduction to certificate authority: The alternative approach for secure transmission of publics key is certificate authority (CA) is firstly defined by Kohnfelder [KOHN78] which can be used for the exchanging the public key without contains the public key authority. The scenario is described in fig.4

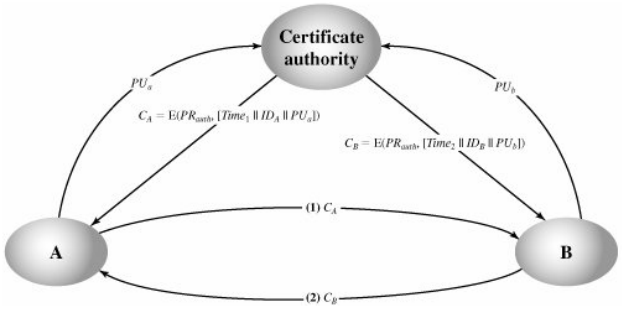
Certificate authority
PU_a
PU_b
C_A = E(PR_{auth}, [$Time_1$ ‖ ID_A ‖ PU_a])
C_B = E(PR_{auth}, [$Time_2$ ‖ ID_B ‖ PU_b])
(1) C_A
A
B
(2) C_B

Figure 4

Algorithm is as follows

1-**PU $_a$ & PU $_b$:** by which each and every system in network can store its public key to the certificate authority.

2- **C_A = E (PR$_{auth}$, [T||ID$_A$||PU$_a$]):** i.e. a certificate generate by the certificate authority to the initiator A for communication with other system in network.

3- **C_B = E (PR$_{auth}$, [T||ID$_B$||PU$_b$]):** i.e. a certificate generate by the certificate authority to the initiator **B** for communication with other system in network.

In this way with the help of CA and CB both the initiator and responder can communicate with each other without sharing the public key and nonce. It can communicate only with the help of the certificate generated by the certification authority (CA).

2. Benefits of using the certification authority [KOHN]: the use of certification authority (CA) provides the following benefits over the public key authority without Certification authority (PKAwCA).

1-In the network each and every participant can determine the identity and the public key of of owner of certificate.

2-Verification can be done by intended participant.

3- The generation, modification and updating only can be done by the certification authority.

4- Participants can identify the time limit and session for every certificate [DENN83].

3. Our Work: The system participate in the communication can trust certificates issued by the CA which contain the identity of every user also some attributes like the employee code, name and department if we talk about any business process for uniquely identification of user. By the CA users can trust the key belongs to the entity specified by the attributes, and that the key can be used safely in the manner for which it was certified by the CA. the comparison against any business process can be done by the following way. (Table 1)

Table 1

Sr. No.	Approach	PKAwCA	CA
1	Key Backup	Key back is not possible as the authority never stores the keys it only sends to the corresponding request.	Yes, it is possible as all keys are stores in the certification authority.
2	Key Pairs	Key pairs are required as there is double encryption first with the authority and second by initiator or responder which increases the complexity.	There is no need of pair of key as only one key is require to encrypt the certificate which reduces the complexity.
3	Key Update, management and History.	Not possible as no record saved.	Possible as each and every key is store with the certificate.
4	Cross- Certification	Not possible as direct communication start after receiving the public key of responder. (Use only for single communication).	Possible as the certificate can be used for further communication.
5	Certificate Repositories and Distribution.	Distribution not possible.	Repository is a service that allows for distribution of certificates. The CA works for issuing certificates to users, Certificate repositories store certificates so that applications can retrieve them on behalf of users.
6	Client-Side Software	There is no client side software for PKAwCA for checking the control over network.	The client side software is available for automatically checking the controls to a certificate, renewing, providing the interface to the key backup, key history and dealing with all the other issue with keys and certificates.

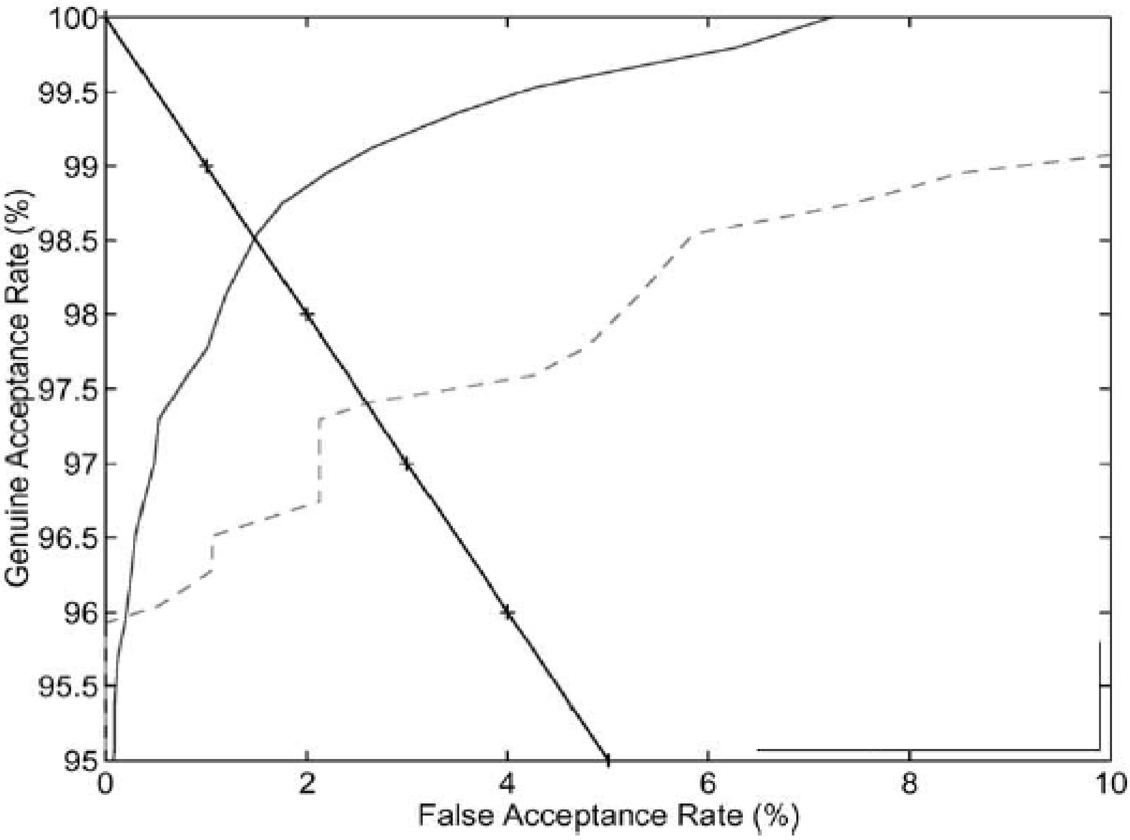

Figure 5

4.Result:

In the work proposed six above mentioned approaches taken by which a graph can be genrated for the
genuine acceptence and false acceptence of key genrated by PKAwCA and CA on the responder or client side. In the following figure (Fig. 5)

——— Represent the keys genrated by the certificate in CA

— — Represent the keys genrated by the PKAwCA

—+— Represent equal error range(i.e. the area in which both approaches give same result)

5. Conclusion:

As certification authority is also work on the basis of public key authority but in the business prospective and for the secure communication over the network it is beneficial to user to adopt the technique for certification authority. The main purpose of PKA is to provide the trustworthy networking and communication environment. This goal can be better achieved by providing the certificate to participants with the help of CA which enables encryption and digital signature possibilities over the channel.CA helps many of the necessary functions to achieve an automatic control like key backup, cross verification and key updating, management etc and give the better interaction with the client-side software. The result also shows that it is genuine accepter of every key with all constraints.

6. References:

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice,* 2da. Edition, Prentice Hall, New Jersey, 1999

[2] "New Public Key Authentication Frameworks with Lite Certification Authority Xiaolei Dong, Licheng Wang, and Zhenfu Cao

[3] [FBCA] W. T. Polk and N. E. Hastings, *Bridge Certification Authorities: Conecting B2BPublic Key Infrastructures.* NIST 2001 http://csrc.nist.gov/pki/documents/B2Article. Pdf

[4] "A Method for Obtaining Digital Signatures And Public-Key Crypto Systems" by R.L. Rivest, A. Shamir, and L. Adleman

[5] William E. Burr, *Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations*. Federal Public Key Infrastructure Technical Working Group, Washington, D.C., September 1998. Available at http://csrc.nist.gov/pki/twg/welcome.html

[6] N. Ferguson; B. Schneier (2003). *Practical Cryptography*. Wiley. ISBN 0-471-22357-3.

[7] J. Katz; Y. Lindell (2007). *Introduction to Modern Cryptography*. CRC Press. ISBN 1-58488-551-3.

[8] Branchaud, Marc, "A Survey of Public-key Infrastructures", Department of Computer Science,McGill University, Montreal, 1997

[9] Netscape, "Introduction to Public-Key Cryptography",http://developer.netscape.com/docs/manuals/security/pkin/contents.htm

[10] Curry, Ian, Entrust Technologies, "Getting Acquainted With Entrust/Solo and Public-key Cryptography", version 1.0, July 1997