RESEARCH ARTICLE OPEN ACCESS

Data Transaction Secure Information Sending to Authentication Side

M.Senthil Murugan
Head & Assistant Professor, Dept.of Computer Science, Immaculate College for Women, Viriyur.

Abstract:

We sent a message or data to that particular authenticate claims in secured manner using some key certificate for each data. It means if we send a message to certificated Author but he should not present there to receive data. In that case, unauthorized person could able to hack that data. By the usage of PKI (Public Key Infrastructure) key certificate format the unauthorized people can't access this typical PKI key format. So we introduced these keys format for each data while we sending and receiving the message.

Keywords: CA, PKI, Cryptography, Personal CA.

I. INTRODUCTION

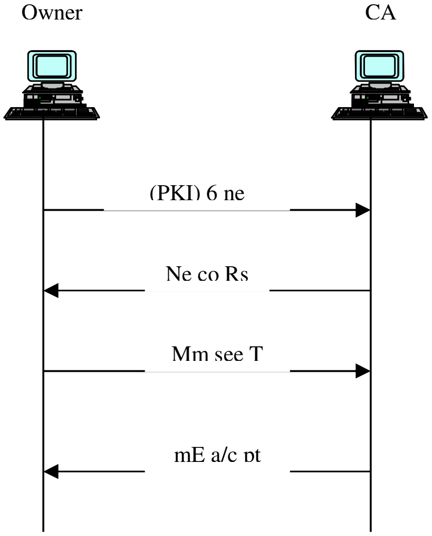
Imagine that we have been asked to design a certification process for our organisation from scratch. In other words, the organisation has identified a need for a PKI that results in every employee having a public key certificate that contains the employee's public key for internal use only within the organisation. The owner is placed in full control of their own key material. It may be easier and more secure to manage the generation of key material centrally. The certification process might appear more seamless to the owner. The owner needs to prove to the CA that they actually know the private key before the certificate can be issued. The owner must trust the CA to securely deliver the private key to the owner and to dispose of it afterwards. However registration is done, there is one very important check that must be performed before proceeding with the issuing of a public key certificate – that the owner actually knows the private key corresponding to the public key in the certificate. If the CA does the key generation then this problem does not arise, but if the owner generates the key pair then this check is essential.

- Public key infrastructures 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 of which 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 recognised standards and best practice procedures that encourage interoperability between different CAs and PKIs.

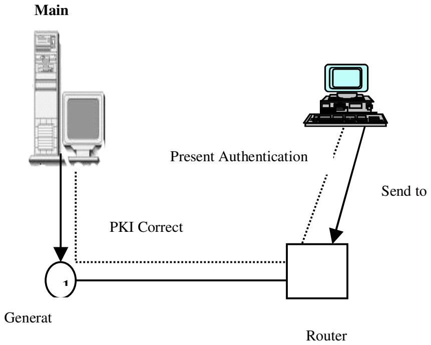
- There are alternatives to traditional PKIs, but these come with their own problems and are most likely to be favoured in niche application areas.

II. KEY AGREEMENT:

- Feature Exchange:
  - Exchange the features generated at each sensor to identify the common ones.
- Generate Keys:
  - Choose common features and form key.
- Verification:
  - Verification of the key

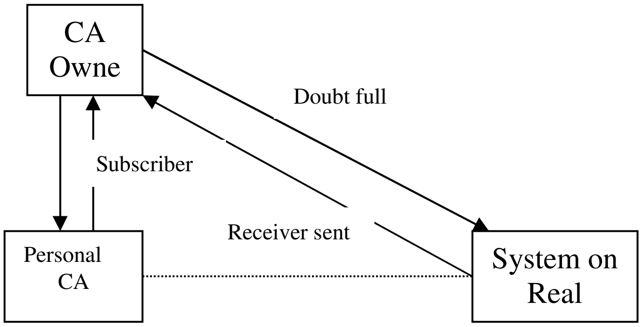


2.1 Basic Process:



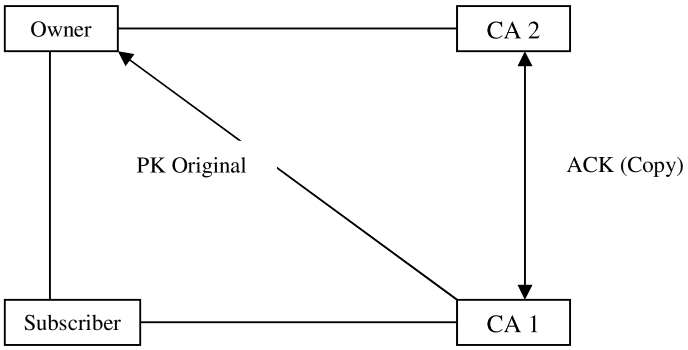
The main systems send the data to the note by the way PKI key well generate and it's send to the router. The router checks that node is to be in online or offline. If it's in am online the data be transferred.

2.2 Subscriber (CA) Usage:



Subscriber checks that node it's being in an offline or online. And it is in an online it intimate on owner "The particular node is read to receive data".

2.3 Four Transactions:



The transaction being held with the owner ,CA1, and CA2.The owner wants to transfer the data to CA1.The CA2 would communicate that information to CA1.The CA1 also send acknowledgement to CA2, " Iam ready to receive" , then the owner will directly send the data to CA1.

III. CONCLUSION:

We propose the PKI key is used to transfer the data with high security. Because the owner will send the data to CA1, CA2 they both known about the PKI only we start transaction between them, otherwise not. If CA2 also can’t able to receive the data from CA1.

Authentication
+
Secure communication
=
Good Transaction

The owner would control all the process. Without the knowledge of owner CA1 and CA2 also can’t communicate. If any one in offline the data will not transfer in that case we introduce subscriber. It work is to check whether CA1 or CA2 is being in online or offline and send that information to the owner. For that reason unauthorized people can’t hack or shawl our data. So that we say PKI key format is best for transactions.

REFERENCES:

[1] William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan, “Your 802.11 Wireless network has No clothes (March 2001),” http://www.cs.umd.edu/~waa/wireless.pdf

[2] Avi Freedman, Zion Hadad, “Handoff Schemes Overview and Guidelines for handoff Procedures in 802.16,” IEEE C802.16sgm-02/24, 2002.

[3] Matthew S. Gast, *802.11 Wireless Networks: The Definitive Guide*, O’Reilly, 2002.

[4] Kihun Hong, Souhwan Jung, Ki Jun Lee, Brian Lee, Jungwook Wang, “Secure Roaming of Key Association for Fast handover,” IEEE C802.16e-04/407, 2004.

[5] David Johnston, Jesse Walker, “Overview of IEEE 802.16 Security,” *IEEE Security & Privacy*, May/June 2004.

[6] Richard R. Joos, Anand R. Tripathi: Mutual Authentication in Wireless network (June 1997); http://cs.engr.uky.edu/~singhal/CS685-

[7] Kyung-ah Kim, Chong-Kwon Kim, Tongsok Kim, “A seamless handover Mechanism for IEEE 802.16e Broadband Wireless Access,” International Scientific-Practical Conference (ISPC) Communication-2004, August 2004.

[8] Changhoi Koo, Sohyun Iim, Jungje Son, “Inter-BS communication for IEEE 802.16e handoff,” IEEE 802.16e-03/29, 2003.

[9] Jeff Mandin, 802.16e Privacy Key Management (PKM) version 2, IEEE C802.16e-02/131r1, 2002.

[10] Wenbo Mao, *Modern Cryptography: Theory and Practice*, Pearson Education, Prentice Hall PTR, 2004.

[11] Roger Marks, “A technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access,” IEEE C802.16-02/05, 2002.

[12] Ron Olexa, *Implementing 802.11, 802.16 and 802.20Wireless network*, ELSEVIER, July 2004._

[13] Kaveh Pahlavan, Prashant Krishnamurthy, *Principles of Wireless Networks: A unified Approach*, Pearson Education, Prentice Hall PTR, 2002.

[14] William Stalling, *Cryptography and Network Security: Principles and Practices, 3rd edition*, Pearson Education, Prentice Hall PTR, 2003.

[15] Daniel Sweeney, *WiMax Operator Manual: building 802.16 Wilreless Networks*, Apress, 2005.

[16] Feng Tian, DongXin Lu, Rui Li, “Comment on Security Roaming of Key association for Fast Handover,” C802.16e-04/571r1, 2005.