2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

A study on the AC and PMI model for the Defense computer network

H.S. Yoon*, S.C. Kim*, J.S. Song*
*Dept. of Computer Science, Yonsei University
e-mail : yoon@emerald.yonsei.ac.kr

Abstract

This paper is a study on the AC and PMI model for the defense computer network. It is suggested that the organization plan of PMI model is a proper model for the characteristics of military system and military defense network security demands based on defense PKI system. Futhermore, it will be presented both various types of defense AC and AC according to the role and clearance in PMI.

Defense AC will provide strong users' authentication and Role Based Access Control to give more secured and trusted authentication service by using users' attribute such as role and clearance.

1. Introduction

In E-commerce through the open internet, public key cryptosystem is used as core technology since it has the function of confidentiality, integrity, authentication, non repudiation. PKC is used in PKI, and it only verifies one's identity, but can't support attribute information such as users' authority, duty, status, etc..

Recently, providing users' attribute information, we are studying AC which is combined authentication system with privilege management system to complement the limited function of PKC. This infrastructure that is issuing, storing and managing AC is PMI.

This paper presents models for Defense computer network based on AC with the model of defense PMI. Also it suggests defense AC which can provide various users' attribute information like AC according to role and clearance based on the most suitable role model for the military authorities.

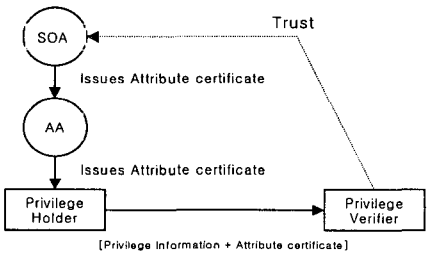
This paper begins as follows :

A quick introduction to PMI and AC is given in section 2. The consideration of Defense computer network and Defense PKI is presented in section 3. Military PMI model architecture and the definition of suitable AC are discussed in section 4. Finally, section 5 contains the conclusions and the future work.

2. Preliminaries

2.1 Definition of PMI

PMI is the infrastructure for issuing, storing and managing AC, and it is the structure which CA guarantees and maintains between resource related with authority and the privilege holder. This is the figure of general PMI structure as below.



(Fig 1) PMI structure

2.2 Basic elements

(1) SoA(Source Of Authority) : It is trusted by a privilege verifier as the enuty with ultimate responsibility for assignment of a set of privileges. An SoA is equal to 'root CA' in the PKI.

(2) AA(Attribute Authority) : An authority which

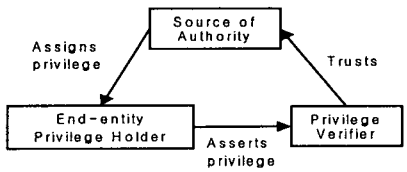
assigns a privilege by issuing attribute certificates. It is analogous to 'CA' in the PKI.

(3) Privilege Holder : A privilege holder using their attribute certificates or public key certificate to assert a privilege. It is analogous to 'End-entity' in the PKI.

(4) Privilege Verifier : An entity verifying certificates against privilege policy. It is analogous to 'relying party' in the PKI.

2.3 PMI models

In ITU-T documents, it is presented several applicable models such as general, control, delegation, and role model in PMI[1]. The following figure shows the general model.



(Fig 2) General Model

2.4 Attribute Certificates

To provide attribute information, we can use extended fields of X.509, smart certificate, and PKC linked to AC. The standard profile of AC is started in both IETF and ITU-T[1,2].

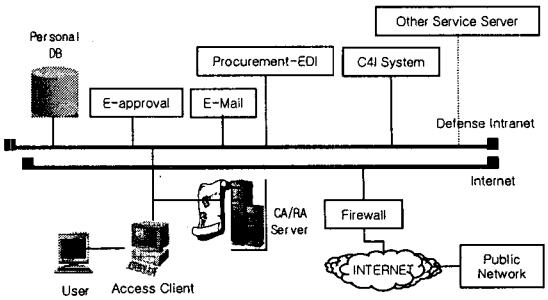
They give the same basic field definition but define attribute field and extended field in a little difference. IETF documents define access identity, charging, group, role, clearance, etc. in the attribute field of AC[2].

3. Defense computer network and PKI

3.1 Architecture of Defense computer network

Defense computer network is managed by Intranet through Defense WAN and Internet using the internet network through ATM WAN.

Defense intranet is composed of electronic approval system, E-mail system, C4I, and Procurement-EDI. The figure 3 shows the architecture of Defense computer network.



(Fig 3) Architecture of Defense computer network

3.2 Threat and ITSEC

(1) Threat

In the system of sending/receiving document files, it can't be guaranteed integrity and confidentiality of sending/receiving document files without encrypting data and military defense intranet access has weak authentication such as personal ID and password causing of being exposed on the network easily. Also it can't be protected in the insiders' threat and hacking.

(2) ITSEC

Building a security operation system to the required level in Defense computer network, there are some requirements as below.

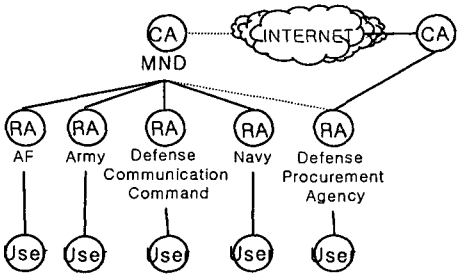
<Table 1> Contents of security requirement

Category	details
certificate/ authentication	certificating each other when they communicate
accountability/ audit	ability of audit who, when, and what did
access control/ authorization privilege	accessing of specific resource can be authorized to permitted entity
exchanging data safely	confidentiality, integrity, authentication, non repudiation
time stamping	implementing non repudiation with adapting time Stamp

Defense computer network is managed security operation system by C2 level, and it is an integrated solution to solve the above ITSEC with accepting public key using PKI and PMI system.

3.3 Defense PKI

Defense PKI sets Military of National Defense as CA, and it will have a model which consists of four RA's in nationwide[3].

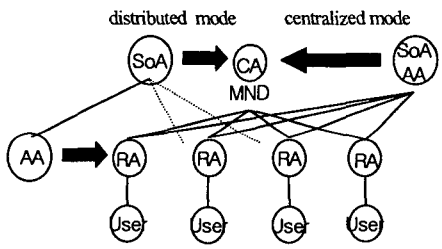


(Fig 4) Defense PKI

4. Organization plan of Defense PMI model

4.1 Centralized Mode vs. Distributed Mode

It is divided a centralized mode and a distributed one where to set SoA and AA.



(Fig 5) Centralized vs. Distributed Mode

(1) Centralized Mode

This mode is a model that sets SoA and AA inside of MND. It gives an advantage for the management of attribute authentication and security because it manages every work related to AC in the center.

(2) Distributed Mode

This mode is a model that sets SoA in MND then sets AA in each RA. SoA can be connected to external CA through the Internet, and in the intranet it controls local AA and also delegates some privilege to it. AA gives proper attribute information to each army. It can be very flexible to apply delegation model or role model properly according to role circumstances and situations. The characteristics of each mode is shown in Table 2.

<Table 2> characteristics of the modes

Category	characteristics
Centralized mode	- centralization of work to MND - centralized management and easy to keep security - easy to frame a unified policy
Distributed mode	- providing proper AC to each army - SoA be able to delegate and control AA - flexible to apply delegation model or role model

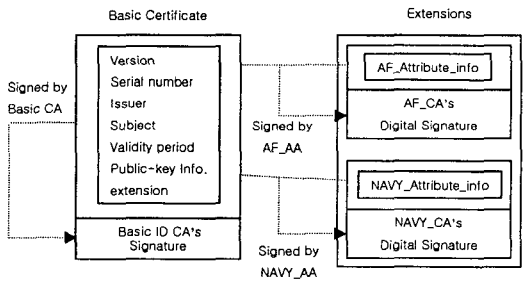
4.2 Defense AC

(1) Using extended fields of X.509

There is a simple way to use SubjectDirectoryAttributes extension fields of X.509. It can be used without any changes of existing PKI, but has serious problems such as lifetimes that do not match the validity period for a PKC and incongruence authentication information for authentication subject.

(2) Smart Certificates

Users' attribute information can be provided by Joon S. Park & Ravi Sandhu's smart certificate[4]. The following figure is the example of smart certificates which can provide users' attribute with Monolithic Signature, and defense AC can be offered as below.



(Fig 6) AC applied smart certificate

Defense AC includes attribute information issued by AA in extended fields of PKC. The characteristics of the AC is as follows :

① Public key and the attribute can be maintained independently.

② Basic certificate is expired, then all the attributes are meaningless.

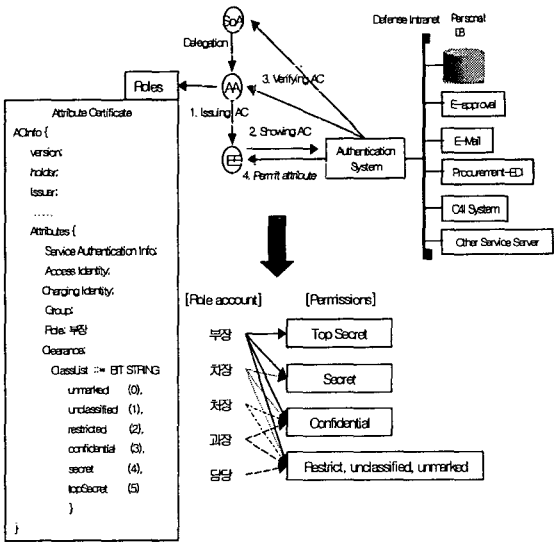
③ Certificates can be issued for specific period.

④ Access control can be made by attributes.

(3) AC according to the role and clearance in PMI

In section 4.1, Defense PMI model can be established as hybrid model of role and delegation model. Also, there are some possibilities to occur ACRL increasing because users' AC is renewed frequently by the change of their status. The efficient method to solve the problem is to decrease re-issuing, changing, and revoking of AC by using of RSC(Role Specification Certificate).

RSC allocates specific privileges for each role. Without any changes of individual AC, it can be modified users' role with ease. RSC is assigned rank, status, and department. Figure 7 shows the hybrid model of defense PMI and it gives an example of access control by using AC.



(Fig 7) Example of applying access control by clearance

(4) Access control scenario

① Issuing AC : AC is issued to users. And then users' role is allocated.

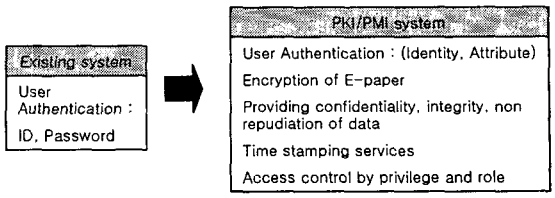
② Showing AC : Users show their AC.

③ Verifying AC : An Authentication system verifies validity of users' AC through the directory server.

④ Permit attribute : An Authentication system authorizes access according to users' privileges.

4.3 Comparisons with existing system

Figure 8 depicts comparison with an existing system and PKI/PMI systems.



(Fig 8) Comparison with existing system

5. Conclusions and future work

In this paper, defense PMI model and defense AC have been presented. Defense PMI model has been divided a centralized mode and a distributed one by where to establish SoA and AA with the model of defense PKI. Moreover, there have been given three types of defense AC which are extended fields of X.509, smart certificates, and PKC linked to AC.

We need the study of more detailed PMI model, real implementation of AC, and verifying of certificate through practical using. Also, the further study will be required that can give users convenience by using SSO(Single Sign On) applied to EAM solution.

References

[1] ITU-T, Draft Revised ITU-T Recommendation X-509(2001E): "Information Technology Open Systems Interconnection - The Directory : Public-Key and Attribute Certificate Frameworks"

[2] Internet Draft, "An Internet Attribute Certificate Profile for Authorization" IETF PKIX Working Group, Jan, 2001

[3] Y.Y. Hwang, "A study on a CA Model for the Defense computer network", CISC 2000 Proceedings, Vol.10, No1, pp.53-64, 2000.

[4] Joon S. Park, Ravi Sandhu, "Smart Certificates : Extending X.509 for secure attribute services on the web", In Proceedings of 22nd National Information Systems Security Conference, Oct. 1999.