A Smooth Expansion Model for PKI*

Gong Jian[1**] Liu Jianhang[2]
[1]Department of Computer Science and Engineering, Southeast University, Nanjing 210096
[2]Software Center Motorola China, Nanjing Division, Nanjing 210000

Abstract: The expansibility of PKI is expected to have the features that when the amount of user exceeds the system capacity, the users' requirement can still be met by simply expanding the number of PKI entities and management levels, and this expansion should be achieved smoothly from the original system. The upward, downward, and horizontal expansions of PKI are discussed in this paper. A path discovery method is suggested to reduce the effect of PKI expansion to the end-entities, so as to enhance the availbility of PKI services.

Key words: Network Security, Key Certificate, CA, PKI, Path Discovery.

1. Introduction

As PKIs are getting more and more important to the applications on Internet nowadays, many efforts have been made to interconnect the independent PKIs to form a larger infrastructure. Therefore, the extendibility of a PKI is very important when the capacity of the PKI is exceeded. In that case, more CAs and management levels should be added to the PKI to meet users'requirement, and all the users and applications could be migrated to the new infrastructure without interfering their normal works.

To end-entities, there are two types of CA certificate: selfCA certificate and crossCA certificate. The former is used to carry a public key for a CA, and the latter is used to present a trusted relationship to a CA. When CAs in different management domains are concerned, crossCA certificates are required to indicate the trusted relationship between these two CAs. And the involved end-entities should be notified to the new trust relationship in order to build certificate chain needed to access the object in that domain.

Within the current PKI framework, the processing of certificates to an end-entity is all the same. The certificates are all regarded as a part of static configuration to the Personal Security Environment(PSE) of the end-entity, and are loaded when the end-entity is initialized. This method makes the expansion of PKI intransparent to the end-entity. That is, when the inter-domain trust

Received 2000-01-09.
* Supported by National 863 High-Tech Program (863-317-01-04-99).
**Born in 1957, male, Professor, Ph.D.

changes, e.g. the PKI is expended and more CAs are added, the configuration of the end-entity has to be changed statically. In this paper, the upward, downward, and horizontal expansions of PKI are discussed, and a smooth expansion model called “Path Discovery” is suggested. The basic idea of path discovery is to process the two types of CA certificate differently: besides the traditional method, the crossCA certificates can be achieved via path-discovery algorithm dynamically, so that the coverage of the PKI can be extended automatically. By this way, the effect of PKI expansion to the end-entities can be reduced, and its extendibility is improved.

2. The expansion of PKI

PKI can be extended downward, horizontally, and upward. The downward expansion occurs within single PKI management domain. When the exist root CA can not meet users’needs, more subordinate CAs are added to share the tasks. The downward expansion is quite straightforward, and is transparent to end-entities, which can be done as following.

(1) The root CA signs an crossCA certificate to authorize the establishment of a subordinate CA;

(2) The subordinate CA will provide certificate chain to new end-entities who contact it directly;

(3) The old end-entities who should belong to the subordinate CA still contact the root CA for their certificate update at first, and the root CA will return a certificate chain to inform the emergence of new subordinate CA, which will turn these end-entities to that CA hereafter.

The horizontal expansion of PKI is stimulated by the cross-verification of two management domains. An example is given as Fig1. The students of NorthSchool want to access the library of EastSchool, so that the EastSchool issues a selfCA certificate with the subject being EastSchool root CA. At the same time, the ACL of the Library Server will allow all the access request from the users with ou=Graduate and o=NorthSchool,c=CN.

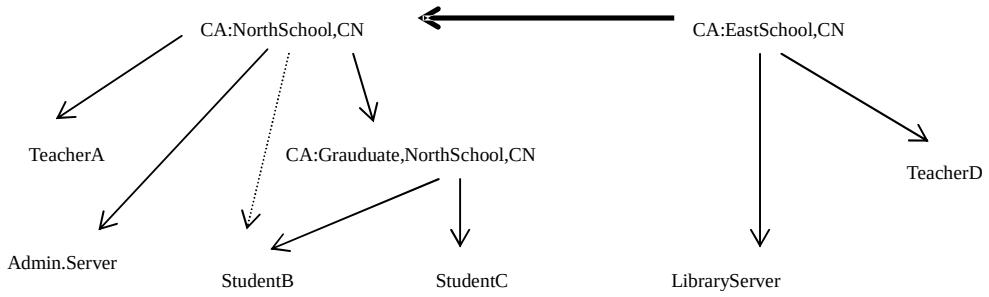

Fig.1 An example of PKI horizontal expansion

On the other hand, if the users in NorthSchool show the CA chain originated from NorthSchool

root CA to the library server in EastSchool as they usually do, the authentication will fail because the server does not know the public key of NorthSchool root CA. Therefore, the users in NorthSchool have to download the crossCA certificate issued by EastSchool root CA to NorthSchool root CA, and put it to the left end of the CA chain when they access to the library server in EastSchool. This kind of horizontal expansion is intransparent, the users are engaged in the trust relationship changes among CAs. If there are other service providers such as WestSchool and SouthSchool, the end-entities have to download all the new crossCA certificates, and change their PSE configuration accordingly. This is quite inconvenient in a large-scale network, and transparent method is expected to make the expansion more smoothly. One possible solution is to let the end-entity know the new chain automatically so that the mutual interference is avoided.

3. Path Discovery

The certificate environment CE of an end-entity includes selfCA certificate set (SelfCACerts), crossCA certificate set (CrossCACerts), end-entities certificate set (EndEntityCerts), one default certificate chain for authentication, and one mapping between certificate chains and their addresses. To enable the path discovery, a path discovery agent is set up for each PKI management domain, which collects and stores all the crossCA certificates that are issued by CAs in other domains with the subject of the certificates being CAs in this domain. With the help of this agent, for the access of end-entity A to B from different domain, the certificate chain verification process can be described as following steps.

(1) A checks first that if B has been visited before, the suitable chain from its mapping table should be showed to B; otherwise its default chain will be showed to B.

(2) B tries to find a selfCA certificate within its SelfCACerts, which can be used as a start point to verify the certificate chain presented by A. If such a certificate is found, the verification can be completed; otherwise, B will return an authentication failure message and its SelfCACerts set.

(3) When receiving a failure message, A will submit B's SelfCACerts to the path discovery agent to let it check if there is any known trusted relationship between this domain and the domains B trusted.

(4) If NULL is returned for the check, the verification is totally failed. If some crossCA certificate returned, A should choose one of them to put it leftmost to the default chain to form a new certificate chain.

(5) A presents the new chain to B, and B will repeat step (2).

(6) If B replies that the verification is successful, A will add the used crossCA certificates to its CrossCACerts, as well as the mapping of address and the new chain to the mapping table for

future usage; otherwise it has to stop the process and discard all the certificates received from B during this process.

Regarding the situation in Fig.1, an example of verification based on path discovery process is showed in Fig.2.

Path discovery agent can be configured to end-entities manually. However, it is better to be notified via a certificate issued by a trusted root CA, and this can be done through the certificate extension field, which is similar to the definition of CRLDistributionPoint. It is reasonable to let the root CA act as the path discovery agent, because for end-entities in a domain, it is the most trustworthy one. As the reliability of the crossCA certificates received by end-entities are guaranteed by the contained digital signature, no extra security consideration is required to the path discovery process. Any attack to the path discovery process, e.g. forgery, will only lead to failure of the authentication instead of a false authorization, so that some ordinary transport protocols, like HTTP and FTP, can be used.

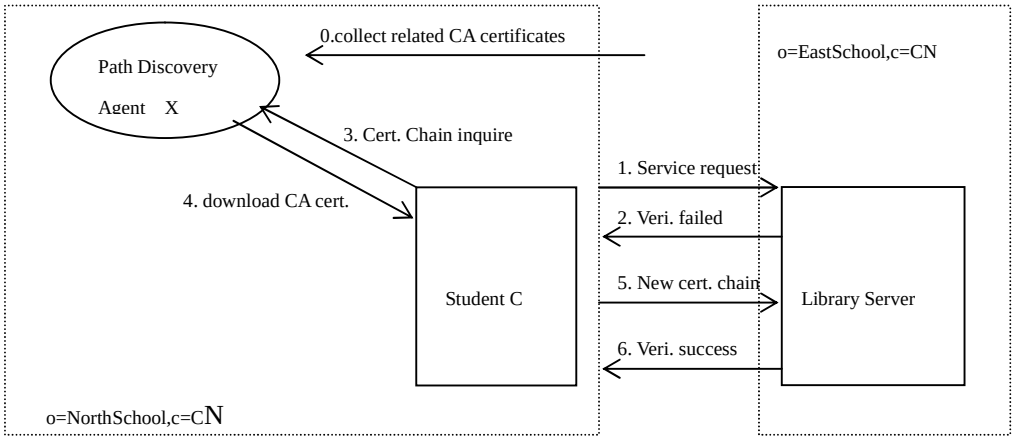

Fig.2 An example of Path Discovery

4. Path Discovery for PKI Upward Expansion

The horizontal expansion of PKIs interconnects different PKI management domains. However, in case that the number of domains is large, maintaining the trust relationship among all the root CAs through issuing crossCA certificates between each other is cumbersome and low efficient. More management levels, i.e. upward expansion, are needed to optimize the situation. As an example showed in Fig.3, when the new root CA which manages the domain Education,CN is established, the PKI is upward extended. The end-entities in the domain can get selfCA certificate and chains originating from the root CA directly. All the certificates that the end-entities got previously can still be used in each subdomain as usual. But when used cross subdomains (within the new domain), these

certificates will face the same problem as in the case of PKI horizontal expansion do. Therefore, the end-entities should download the selfCA certificate of the new root CA and adjust the certificate chains accordingly. By this way, these subdomains can be integrated into a new PKI management domain, and all the services are remained same. For example, suppose student B never uses library server of EastSchool before, and his CE is

SelfCACerts : { (CA:NorthSchool,CN) }

CrossCACerts : { (CA:NorthSchool,CN EE: CA:Graduate,NorthSchool,CN) }

EndEntityCerts:

{ (CA:Graduate,NorthSchool,CN EE:B,Graduate,NorthSchool,CN) }.

The first certificate verification of B to the library server will fail, and B will find two CA names from that domain: CA:Education,CN and CA:EastSchool,CN. Then B turns to the path discovery agent in his domain and gets two crossCA certificates:

(CA:EastSchool,CN EE: CA:NorthSchool,CN) and

(CA:Education,CN EE: CA:NorthSchool,CN).

B can choose one of them and add it to his default certificate chain:

(CA:NorthSchool,CN EE: CA:Graduate,NorthSchool,CN), and

(CA:Graduate,NorthSchool,CN EE:B,Graduate,NorthSchool,CN)

to form a new certificate chain. And this time, the certificate verification will succeed.

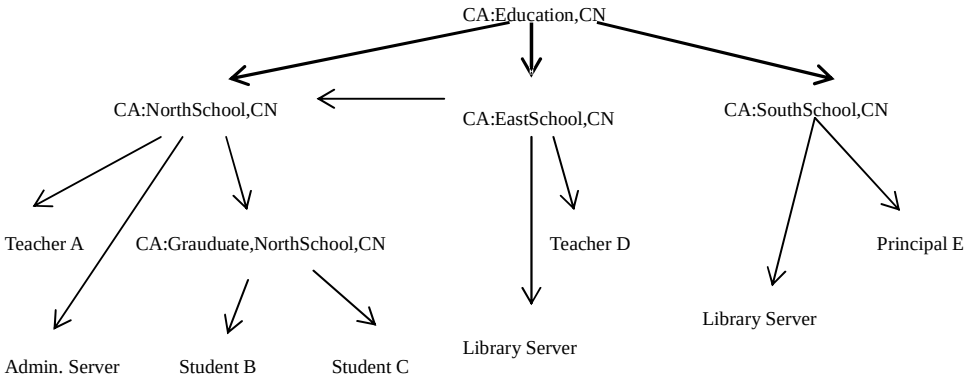

Fig.3 An Example of PKI Upward Expansion

5. Conclusion

Although the basic working mechanisms for CA and end-entities in a PKI management domain are defined quite in detail in the X.509 documents, these PKIs are isolated islands in the real situation. These PKI domains can only be integrated via spontaneous expansion among themselves because it

seems that there will be no such a superpower to coordinate the birth of a global PKI. Generally, there are three kinds of PKI expansion, and two of them are basically not transparent to the end-entities as we discussed above. To improve the efficiency of PKI expansion, and make it smoothly to end-entities, a path discovery mechanism is suggested in this paper, which can help the end-entities to get the correct certificate chains without user interference. The realization of such a mechanism can be combined with the implementation of root CA for a PKI management domain, and can be added to the PSE of an end-entity by its configuration. The process to which the path discovery agent gets crossCA certificates from other domains can be governed by CMP protocol, so that the introduction of path discovery mechanism will not effect the standardization and interoperability of PKIs.

References

[1] Liu Jianhang, CA Based Public Key Management Framework, [Thesis for Master degree], Nanjing: Southeast University, 1999.2

[2] IETF PKIX WG, "Internet X.509 Public Key Infrastructure Roadmap", draft-ietf-pkix-roadmap-00.txt, 1998.9

[3] IETF PKIX WG, " Internet X.509 Public Key Infrastructure Certificate and CRL Profile", draft-ietf-pkix-ipki-part1-08.txt, 1998.6

[4] IETF PKIX WG," Certificate Policy and Certification Practices Framework", draft-ietf-pkix-ipki-part4-03.txt, 1998.4

PKI 的一个平滑扩展模型

龚俭[1] 刘建航[2]

[1]东南大学计算机科学与工程系，南京 210096

[2]中国摩托罗拉公司软件中心南京分公司，南京 210000

摘要 PKI 应具有可扩展性，因此当用户数量超出系统容量时，可以简单地通过增加 PKI 实体数量和管理层次来满足用户的需求，实现从原有系统的平滑扩展。本文讨论了 PKI 的向上、向下和水平扩展等三种方式，提出了一个路径发现方法来减轻 PKI 扩展对端用户所造成的影响，以提高 PKI 服务的可用性。

关键词 网络安全，密钥证书，证书中心，公钥基础设施，路径发现。

中图法分类号 TP393