Proposal to Adapt Reliability of National PKI to Grid Security Infrastructure by Credential Translation and Delegation with OAuth

Daeyoung Heo and Suntae Hwang[*]

Kookmin University, 77, Jeongneung-ro, Seongbuk-gu, Seoul, 136-702 Korea
Tel: (+82) 2-910-4748, Fax: (+82) 2-910-4868
dyheo@cs.kookmin.ac.kr and sthwang@cs.kookmin.ac.kr[*]

Abstract

Grid Security Infrastructure (GSI) is the most common security infrastructure for grid computing, which is also based on Public Key Infrastructure (PKI). Therefore, the process to issue certificates for grid users, which is usually including interviewing with registration authorities (RAs) for identifying the user in person, is complicate and difficult to ensure reliability. We could therefore rely on the certificate issuance process of national PKI, which includes RA system guaranteed by governments. However, it is not possible to adapt the national PKI on GSI without modifying security software due to technical and legal problems. Either certificate validation or certificate path validation will be fail in that case. In this paper, we propose an alternative certificate validation method which translates the original certificate of national PKI to grid credential on separate GSI and delegate the translated credential to grid service by an extended OAuth protocol. The proposed idea is implemented in service called SecureBox which is operating in demo site. GSI can now adapt a reliable certificate issuance process including nationwide RA system from national PKI by the service.

Keywords: *Grid Security, National PKI, Public Key Infrastructure, OAuth*

1. Introduction

Grid computing provides researchers, institutions and organizations with man thousands of nodes that can be used to solve complex computational problems. To leverage collaborations between entities, users of computational grids are often consolidated under very large Virtual Organizations (VOs). PKI is thus adopted in the Virtual Organizations for interoperable authentication among participating institutions. [1, 2]

However, the process to issue certificates for VO users, which is usually including interviewing with RAs for identifying the user in person, is complicate and difficult to ensure reliability. In addition, each institution in VO must establish mutual trust relationship between its own PKIs and all issued certificates inconveniently.

In these days, national PKIs are increasingly adopted for e-Governments in the world. For example, Korea also has a national PKI called NPKI (National Public Key Infrastructures). Therefore, we could have a PKI which is as reliable as the government certifies, and rely particularly on the certificate issuance process as it is, which includes RAs who are guaranteed by governments [3].

[*] corresponding author

2. Dilemma of Using National PKI

In this section, we will consider how the reliable national PKI can be adapted on grid without any modification on the GSI [4] software.

2.1. PKI

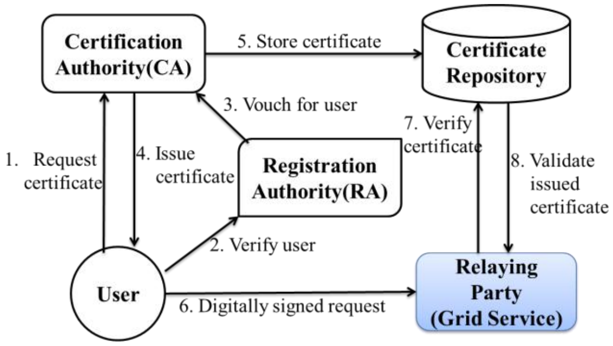
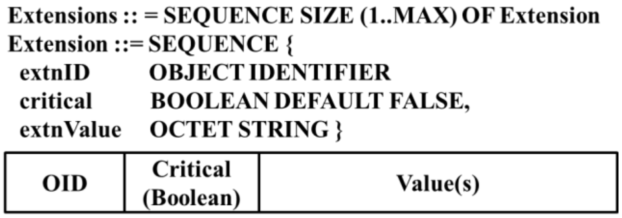


Figure 1. Public Key Infrastructure

A PKI has some fundamental infrastructure components, including certification authorities (CAs), registration authorities (RAs), repositories, and archives. A CA is the basic building block of the PKI. Among other things it supports, a CA acts like a notary to confirm the identities of entities involved in a communication. An RA is an entity trusted by the CA to confirm and validate the identity of users to a CA. This is typically through face-to-face meetings where proof of identity is established. A repository is a database that contains the active digital certificates for a CA system. An archive contains documents and/or revoked certificates related to old or inactive certificates that can be used to settle future conflicts. A typical PKI setup is depicted in Figure 1 [5].

In X.509 standard for PKI, certificate contains pair of public and private keys and also extensible attributes for additional information such as certificate's validation and policy. The additional attributes consist of key, value and criticality as shown Figure 2, and are used for certificate validation [6]. The criticality indicates weather the validation is mandatory or not. When the criticality is set true, validator must know both key and value, and validate the attribute in a known regulated process. If the validator does not know either key or value, the validation is failed.



```
Extensions :: = SEQUENCE SIZE (1..MAX) OF Extension
Extension ::= SEQUENCE {
  extnID      OBJECT IDENTIFIER
  critical    BOOLEAN DEFAULT FALSE,
  extnValue   OCTET STRING }
```

OID	Critical (Boolean)	Value(s)

Figure 2. X.509 Extension Structure

Most grid sites cannot achieve to high reliability because they do not usually operate local RA system due to the cost. If those sites can adapt RA system from existing PKI for example a national PKI, their security infrastructure will be more reliable, particularly in certificate issuance process.

2.2 Dilemma

National PKIs are generally implemented well as shown in Figure 2 unlike most PKIs for grid computing. Particularly, national authority force the process, related with CA and RA, to be observed by law in order to guarantee high level of reliability. Certificate of national PKI technically contains extended attributes for additional information, which usually comply national standard only. Furthermore, the attribute for regulation such as certificate policy is required that its criticality set true.

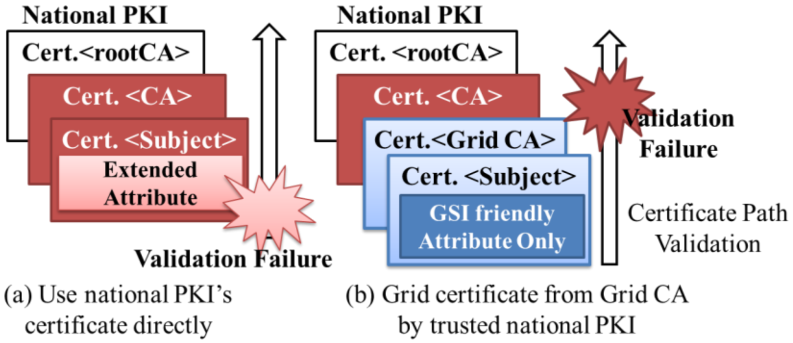


Figure 3. Failure Case of National PKI Validation

There are two ways for adapting a national PKI on GSI. First, certificate of nationwide PKI can be used directly as shown Figure 3(a). In this case, certificate validation will be fail if the certificate includes extended attribute whose criticality set true, because additional keys and values of extended attributes are not known in GSI.

Second, instead of using national PKI's certificate directly, GSI may be authorized by a national PKI and issue new certificate as shown Figure 3(b). Unlike the above situation, certificate validation will be success here because the new certificate will contain information which allowed on GSI. However, certificate path validation will be fail eventually, because CA certificate issued by national PKI contains still unknown information to GSI.

So it seems a dilemma to adapt the reliability of national PKIs on GSI without modifying software. In the next section, we will describe how the certificate chain can be separated with keeping certificate path information and how the path can be validated without modifying GSI software.

3. Certificate Path Validation

To avoid the dilemma described in the previous section, national PKI and GSI are separated in non-hierarchical structure as shown Figure 4. GSI certificate can be validated by the original GSI software with certificate itself and Grid CA certificate only because the certificate path is not directly connected to the one of national PKI. However, the original path of national PKI certificate must be found somewhere in the Grid certificate and validated in any way in order not to damage usual PKI certificate path mechanism.

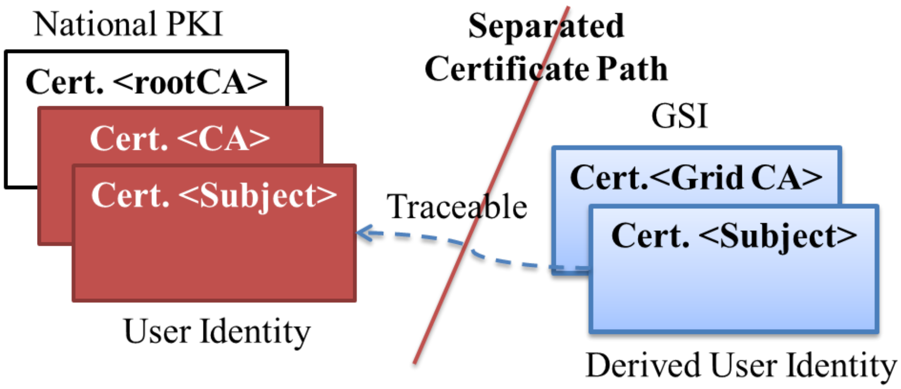


Figure 4. Separated Certificate Path in Non-hierarchical Structure

In this section, we will describe how to store certificate path of national PKI in non-critical part of GSI certificate, and a method of validating the certificate path with the stored information.

3.1. Keeping Original Certificate Path Information

To trace the original certificate path, it must be found via GSI certificate. Four values from the original and CA certificates are required to search and identify the original certificate. Public keys of the original and CA certificate and issuer's name of the original certificate for validating certificate path and issuer's name is used for searching the original certificate. The original certificate is searched by subject name. These values are stored in optional X.509 attributes of a new certificate issued in GSI, as shown in Figure 5.

First, subject name of the original certificate is stored in 'subject alternative name' of new GSI certificate because subject name of each certificate must be unique in PKI, while issuer's name of the original certificate is stored in 'issuer alternative name' to trace the original certificate path which cannot be traced by PKI regularly because the issuer of the new certificate is GSI, not the national PKI anymore.

Second, public keys of the original and CA certificates are also stored to validate that the searched certificate is used to derive the new certificate. The public key of the original certificate is stored in 'subject key identifier (SKID)' in the form of hashed by SHA-1 algorithm. Information of CA certificate which issued the original certificate is stored in 'authority key identifier (AKID)'. The information may include public key identifier, issuer’s name of CA certificate, and serial number. The public key is also stored in the same form of hashed by SHA-1 like SKID.

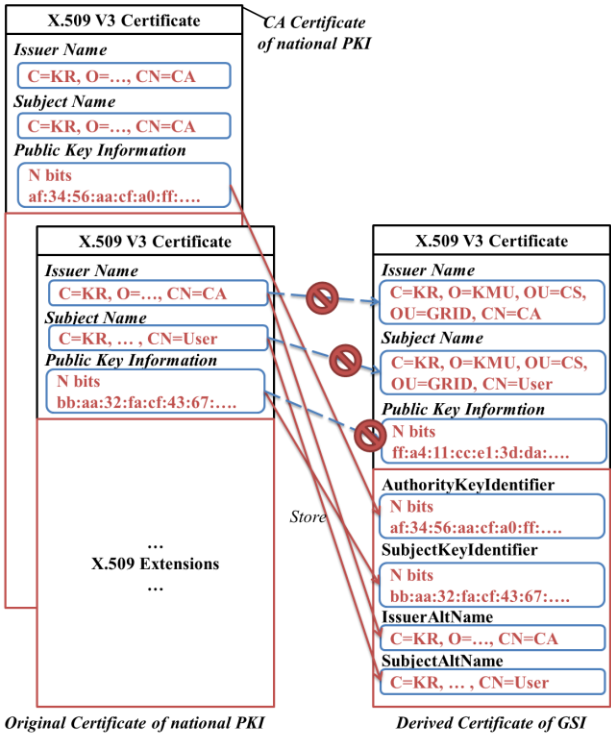


Figure 5. Keeping Original Certificate Path Information

All the above are shown in Fig. 5. And an alternative way of certificate path validation using these stored values will be described in the next section.

3.2 Certificate Path Validation

Certificate validation consists of basic and path validations. [7] Basic validation confirms the valid time and revocation status of user certificate, while certificate path validation does basic validation for issuer's certificates.

As shown in Figure 6, when GSI CA issues a new certificate, it must save the original certificate path in order to reconstruct full certificate path from it for validation of the new certificate. A new alternative certificate path validation algorithm consist of three steps by adding searching step for the original certificate path and verifying step of relationship between user certificate and the original certificate.

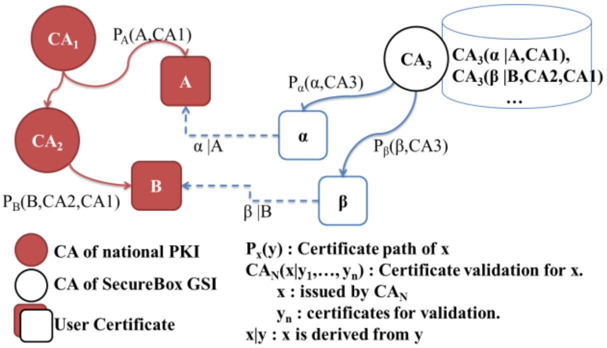
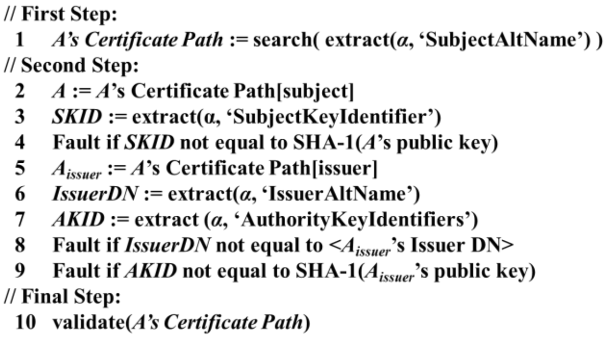


Figure 6. Proposed Certificate Path

In the first step, the original certificate path is searched by 'subject alternative name' from repository which is managed by CA. In the second step, it is verified that the user's certificate of GSI is derived by the original national PKI certificate. This verification is made by comparing SKID of user certificate with the public key of the original national PKI certificate, and AKID and public key of the issuer of the original certificate. In the last step, the original certificate path rebuilt in the first step is validated. Figure 7 shows the validation algorithm in detail.



```
// First Step:
    A's Certificate Path := search( extract($\alpha$, 'SubjectAltName') )
// Second Step:
    A := A's Certificate Path[subject]
    SKID := extract(α, 'SubjectKeyIdentifier')
    Fault if SKID not equal to SHA-1(A's public key)
    $A_{issuer}$ := A's Certificate Path[issuer]
    IssuerDN := extract($\alpha$, 'IssuerAltName')
    AKID := extract ($\alpha$, 'AuthorityKeyIdentifiers')
    Fault if IssuerDN not equal to <$A_{issuer}$'s Issuer DN>
    Fault if AKID not equal to SHA-1($A_{issuer}$'s public key)
// Final Step:
    validate(A's Certificate Path)
```

Figure 7. Validation Algorithm of Proposed Certificate Path

4. SecureBox: Grid Identity Service

In this section, we will describe a grid identity service called SecureBox which is implemented based on the alternative certificate path validation method described in the previous section. SecureBox allows users to login to original GSI of grid by national PKI certificate.

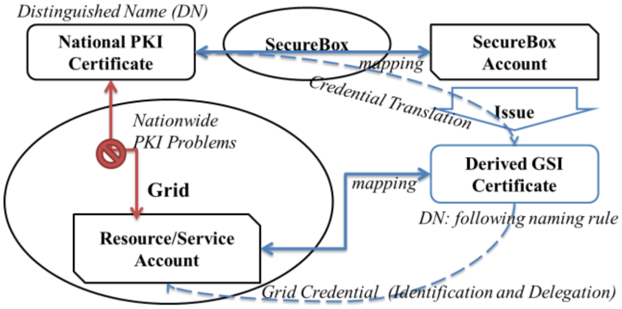


Figure 8. Identity Mapping Among National PKI, SecureBox and Grid

As shown in Figure 8, SecureBox translates the identity of national PKI to a grid credential, and delegates the credential to grid service. SecureBox is also managing effectiveness of certificate by checking its revocation status periodically.

4.1. Grid Credential Translation

SecureBox translates national PKI certificate to GSI certificate by the following three steps: First, national PKI certificate is registered to account of SecureBox by mapping those names. Second, a new GSI certificate is issued as shown in Fig. 6, when user login by national PKI (either original or reissued one) certificate first time. The GSI certificate has the same valid time as one of the original national PKI certificate. Whenever a GSI certificate is issued, the original certificate path is saved in SecureBox for future validation. Last, a new grid credential is generated after validation as described in Section 3.2 when login to SecureBox is successful by national PKI certificate. The credential also includes delegation mechanism to allow grid service to use other grid service on behalf of the user.

If the translation is fail due to revocation or reissuance of the national PKI certificate, SecureBox updates CRL by revoking the derived GSI certificate in order to cancel delegated credentials before.

Revocation of the original national PKI certificate cannot be detected unless translation occurs by a new login. So, SecureBox validates the original certificates periodically by background job when service is not busy.

4.2 Grid Credential Delegation

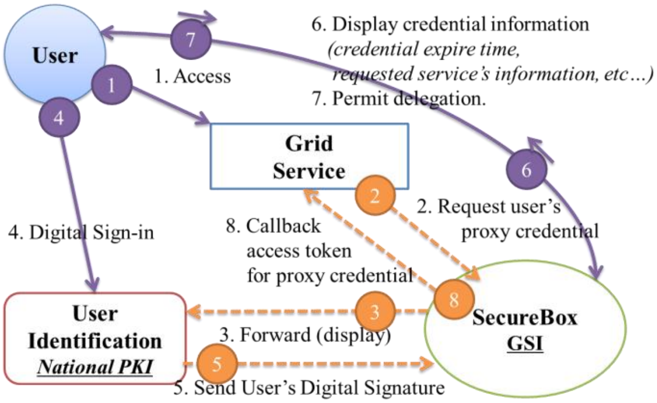


Figure 9. Overall Delegation Process via OAuth

After the translation to grid credential, it will be delegated to grid service. Figure 9 shows the whole process of delegation in detail, which include user's login to SecureBox by national PKI certificate (step 1 ~ step 5), translation to grid credential, and delegation to grid service via extended OAuth protocol [8] (step 6 ~ step 8) which is modified for this purpose by us. The national PKI credential generated by login is translated to grid credential as shown in Figure 5, and validated by the algorithm in Figure 7 between step 5 and step 6.

5. Similar Works

Because we assume that existing secure software be used as it is without any modification, our effort is almost unique. But we introduce most similar works to ours in this section.

5.1. Bridged Certificate Authority

Bridge Certification Authority (BCA) [9, 10] is used to bridge multiple hierarchical CAs. The BCA provides the means to leverage the capabilities of existing corporate PKIs, and is usually based on cross-certificate. In cross-certification, CA from different PKI domains certify to each other, so that relying parties are able to establish trust paths for certificates in remote PKI domains without changing their trust anchor configuration.

If BCA is built by setting cross-certificate between GSI CA and national PKI for our purpose, national PKI certificate can be validated in grid. However certificate path validation will be fail by original GSI software because the path includes national PKI certificate.

5.2. OAuth-based Proxy Delegation Service

In this research, an online credential repository service is proposed to provide authentication mechanism to grid web application based on standard web technology. [11] This service support to grid authentication based proxy delegation between grid service and standard web application. In this service, the X.509 proxy delegation process [12, 13] is added to OAuth [14] protocol for credential exchange, and authentication can be done by an external service such as OpenID [15].

However, this service performs delegation in a single PKI only. So, this research is not fit for our purpose as shown in Figure 3(a).

6. Conclusion

In this paper, we propose a service for adapting reliability of national PKI to GSI without modifying any part of security software by introducing an alternative method of certificate path validation in non-hierarchical structure.

The service called SecureBox is implemented and a demo site is operating currently. It uses an extended OAuth protocol to delegate grid credential in safe way, and certificate translation algorithm and PKI function such CA are added on top of the work in [11].

We believe that the proposed service elevates the reliability level of grid computing by allowing it to use the certificate issuance process of national PKI as it is, in which it is usually difficult to keep reasonable reliability due to management of human resource, registration authorities.

Acknowledgement

This work was supported by research program 2012 of Kookmin University in Korea.

References

[1] M. Pala, S. Cholia, S. A. Rea and S. W. Smith, “Federated PKI Authentication in Computing Grids: Past, Present, and Future”, **(2011)**, pp. 155-164.

[2] I. Foster and C. Kesselman, “The anatomy of the grid: Enabling scalable virtual organizations”, Int. J. High-Perform. Comput. Appl., vol. 15, **(2001)**, pp. 200-222.

[3] D. Patsos, C. Ciechanowicz and F. Piper, “The status of National PKIs – A European overview”, J. Information Security Technical Report, vol. 15, **(2010)**, pp. 13-20.

[4] I. Foster, C. Kesselman, G. Tsudik and S.Tuecke, “A Security Architecture for Computational Grids”, Proceedings of the ACM Conference on Computer and Communications Security, **(1998)**.

[5] W. Jie, J. Arshad, R. Sinnott, P. Townend and Z. Lei, “A Review of Grid Authentication and Authorization Technologies and Support for Federated Access Control”, ACM Computing Surveys, vol. 43, no. 2 Article 12, **(2011)**.

[6] R. Housley, W. Polk, W. Ford and D. Solo, “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile”, **(2002)**, IETF RFC 3280.

[7] R. Housley, W. Polk, W. Ford and D. Solo, “Internet X.509 Public Key Infrastructure: Certificate and CRL Profile”, **(1999)**, IETF RFC 2459.

[8] D. Heo, S. Hwang and K. Jeong, “An Extended OAuth Protocol For X.509 Proxy Certificate Delegation”, (In Korean), J. KIISE: Computer Systems and Theory, vol. 38, no. 5, **(2011)**.

[9] G. L. Millan, M. G. Perez, G. M. Perez and A. F. G. Skarmeta, “PKI-based trust management in inter-domain scenarios”, J. Computers and Security, vol. 29, **(2010)**, pp. 278-290.

[10] J. Huang and D. Nicol, “A calculus of trust and its application to PKI and identity management”, Proceeding of the 8th Symposium on Identity and Trust on the Internet, **(2009)**.

[11] D. Heo and S, Hwang, “OAuth-based Proxy Delegation Service”, ICONI, **(2011)**, pp. 189-193.

[12] S. Tuecke, V. Welch, D. Engert, L. Pearlman and M. Thompson, “Internet X.509 Public Key Infrastructure: Proxy Certificate Profile”, **(2004)**, IETF RFC 3820.

[13] V. Welch, I. Foster, C. Kesselman, O. Mulmo, L. Pearlman, S. Tuecke, J. Gawor, S. Meder and F. Siebenlist, "X.509 Proxy Certificates for Dynamic Delegation", 3rd Annual PKI R&D Workshop **(2004)**.
[14] E. Hammer-Lahav (ed.). The OAuth 1.0 Protocol **(2010)**, IETF RFC 5849.
[15] OpenID, Specifications, http://openid.net/deverlopers/specs **(2007)**.

Authors

Daeyoung Heo

~2004, B.S. Kookmin Univ.(Korea), Dept. of Computer Science.

~2006, M.S. Kookmin Univ., Dept. of Computer Science.

~Now, Ph.D. candidate, Kookmin Univ., Dept. of Computer Science

Suntae Hwang (Corresponding Author)

~1985, B.E. Seoul National Univ.(Korea), Dept. of Computer Science

~1987, M.E. Seoul National Univ., Dept. of Computer Science

~1996, Ph.D. Univ. of Manchester (U.K), Dept. of Computer Science