Delegation using A Proxy Certificate in On-line

Taesung Kim, Sangrae Cho, Seunghun Jin

Electronics and Telecommunications Research Institute,
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350 KOREA
{taesung, sangrae,jinsh }@etri,re,kr

ABSTRACT

Delegation is frequently used in real world. In order to make it possible in on-line, the fact of delegation should be protected from malicious modification and the right of a proxy should be controlled properly. This paper describes security requirements and proxy certificate and proposes a practical method of restriction of a proxy. Finally, the prototype implementation is addressed.

Keywords: delegation, proxy certificate

1. INTRODUCTION

In the real world, delegating the right of signature to a person by an original signer is useful in many situations. Traveling executives can delegate to their secretaries to sign certain documents during their absence. Managers can delegate his privileges to their subordinates to perform certain signature. Subordinates use those privileges for less important and time-consuming tasks such as signing procedural documents routinely. However, there are many difficulties to be overcome before applying this delegation procedure for existing computing environment with a current X.509 digital certificate. To delegate the power of signature, the owner of a certificate should give a private key and encryption password for the private key to a proxy signer. This solution has many security problems. The private key can be misused to sign for tasks, which the owner did not authorize. A proxy signer can repudiate the signatures that he wrote previously. Furthermore, he can give the private key to other people or even attackers without the owner's consent. Finally, the chance that the private key can be exposed easily increases dramatically since the private key is shared with many other proxy signers.

IETF PKIX working group proposed the proxy certificate in order to overcome these limits of X.509 certificate. The proxy certificate has additional extensions which have information about delegation. However, the profile of proxy certificate describes only basic method about delegation and it does not have the procedure how to issue a proxy certificate and the method how to restrict privilege of the proxy.

This paper will describe security requirements of proxy signature and introduce the proxy certificate which IETF PKIX proposed. After that, we will propose the mechanism that can restrict privilege of a proxy based a policy and the protocol that enables a third party to trace and identify the original signer for proxy signature validation. Consequently, we designed and implemented a prototype, which can show how the right of signature can be delegated and how the security of proxy certificate can be ensured.

2. REQUIREMENTS OF PROXY SIGNATURE

Security requirements of proxy signature are as follows:

1) Strong unforgeability
A designated signer, called proxy, can only create a valid proxy signature. Therefore it means that even owner of original certificate or any other third party should not be able to create a valid proxy signature.

2) Verifiability
From proxy signature a verifier can be convinced of the original signer's consent and could authenticate identity of the proxy.

3) Strong undeniability
It is difficult for a proxy to repudiate its own signature against any verifier.

4) Protection of misuse
A proxy signature must be used for only privileges and period which original signer specified.

To satisfy first and third requirement a proxy should cre-

ate new public and private key pair for a proxy certificate. The private key is never disclosed to any third party for any reason. If a proxy already has the X.509 digital certificate which is issued from Certification Authority and a public and private key pair, which is the same as the key pair in the digital certificate, is used for creating a proxy certificate, a malicious original singer can insist ownership of signed document which the proxy signed with his X.509 digital certificate. The second requirement points out that a proxy certificate should be signed by an original signer. If the identity of a holder of a proxy certificate is necessary to be identified, then the proxy certificate can contain necessary information. The last requirement suggests that a proxy certificate should be used as it is intended and in any cases the mechanism should be provided to prevent any misuse.

```
ProxyCertInfo ::= SEQUENCE {
    version                 INTEGER (0..MAX),
    pC                      BOOLEAN DEFAULT TRUE,
    pCPathLenConstraint     INTEGER (0..MAX) OPTIONAL,
    proxyRestriction        ProxyRestriction OPTIONAL,
    proxyGroup              ProxyGroup OPTIONAL,
    issuerCertSignature     Signature OPTIONAL }

ProxyRestriction ::= SEQUENCE {
    policyLanguage          OBJECT IDENTIFIER,
    policy                  OCTET STRING }

Signature ::= SEQUENCE {
    signatureAlgorithm      AlgorithmIdentifier,
    SignatureValue          BIT STRING }

ProxyGroup :: = SEQUENCE {
    proxyGroupName          OCTET STRING,
    proxyGroupAttached      BOOLEAN DEFAULT TRUE };

DelegationTrace ::= CHOICE {
    x509                    [0]   X509DelegationTrace }

X509DelegationTrace ::= SEQUENCE {
    agreedCertInfo          AgreedCertInfo,
    x509AcceptorInfo        X509AcceptorInfo }

AgreedCertInfo ::= SEQUENCE {
    ignoredExtensions       SEQUENCE OF OBJECT IDENTIFIER,
    certSubsetHash          Hash }

X509AcceptorInfo ::= SEQUENCE {
    acceptorSig             Signature,
    acceptorName            Name,
    acceptorAltName         GeneralName OPTIONAL,
    acceptorCertHash        Signature }

Signature ::= SEQUENCE {
    signatureAlgorithm      AlgorithmIdentifier,
    signatureValue          BIT STRING }
```

[Figure 1] Extensions of proxy certificate from IETF PKIX

3. PROXY CERTIFICATE

A proxy certificate is a public key certificate with the following properties

1) It is signed by either certificate issued from Certificate Authority or another proxy certificate.

2) It has its own public and private key pair, distinct from any other certificate.

3) It has no distinct identity of its own. The proxy inherits the subject from the original certificate that signed the proxy certificate.

A proxy certificate is a document that has information about the proxy and is signed by original signer. The power of signature is limited by including the term of validity and the privilege of a proxy in a proxy certificate.

The ProxyCertInfo and DelegationTrace are new extensions which are haven only a proxy certificate and not normal certificate. The former indicates whether or not a certificate is a proxy certificate and whether or not the issuer of the proxy certificate has placed any restrictions on its use. The latter is used to provide information about the identity of the proxy and, in some cases, to demonstrate that the proxy has agreed to accept the proxy certificate. ASN.1 of ProxyCertInfo and DelegationTrace is [Figure 1].

The ProxyCertInfo extension indicates whether or not a certificate is a proxy certificate and whether or not the issuer of the certificate has placed any restrictions on its use. If a certificate is a proxy certificate, then the proxyCertInfo extension must be present, the pC field must be true. The proxyRestriction field, if present, specifies restrictions on the use of this certificate. Proxy restrictions are used to limit the amount of right delegated, for example to assert that the proxy certificate may be used only to make requests to a specific server, or only to authorize specific operations on specific resources. Within the proxyRestriction, the policy field is an expression of policy, and the policyLanguage field indicates the language in which the policy is expressed.

The DelegationTrace extension is used to provide information about the identity of the proxy and, in some cases, to demonstrate that the proxy has agreed to accept the proxy certificate. X509DelegationTrace is intended for use when that authentication took place using X.509 certificates. The X509DelegationTrace structure is used to verify that, at the time the proxy certificate was issued, the proxy had agreed to accept it. This structure consists of two required fields: the agreedCertInfo field, which contains hashes of some information related to the certificate, and the acceptorInfo field, which contains the proxy's signature of the agreedCertInfo, plus additional information that can be used by a relying party to verify the proxy's signature.

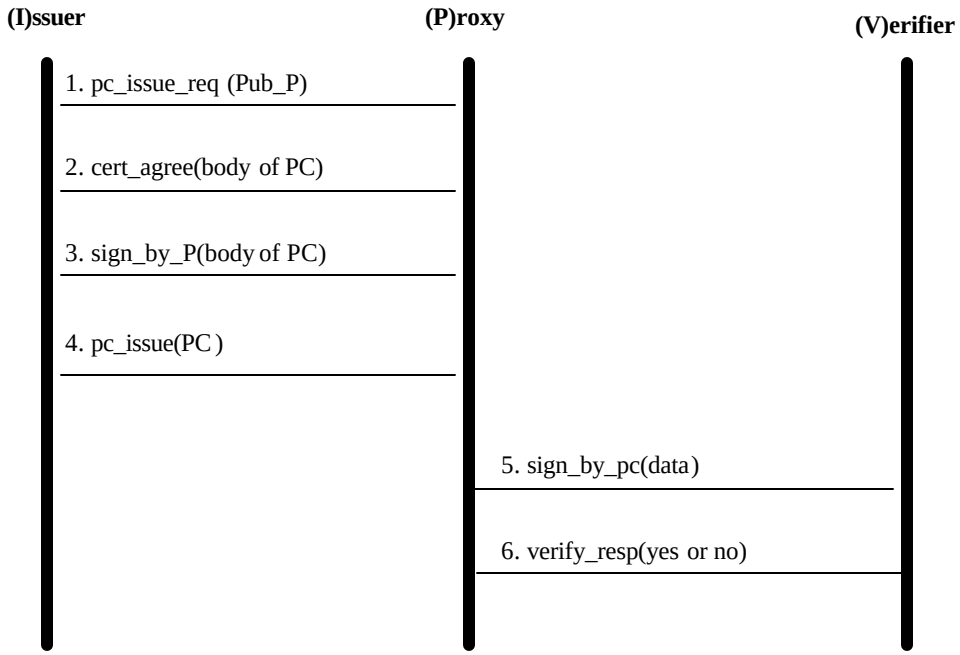
```
EtriPolicyLanguage ::= SEQUENCE {
    period          [0] EtriPeriod OPTIONAL,
    usage           [1] EtriUsage OPTIONAL,
    targetApplication   [2] GeneralNames OPTIONAL
}

EtriPeriod ::= SEQUENCE {
    notBefore INTEGER (0..MAX),
    notAfter   INTEGER (0..MAX)
}

EtriUsage ::= SEQUENCE OF IA5String
```

[Figure 2] ASN.1 of policy language

4. PROXY RESTRICTION

The proxyRestriction field of ProxyCertInfo extension specifies restrictions on the use of the proxy certificate. Proxy restrictions are used to limit the amount of authority delegated, for example to assert that the proxy certificate may be used only to make requests to a specific server, or only to authorize specific operations on specific resources. But the profile of IETF does not define this field. Therefore, each application has to design this field.

This paper proposes the general form for proxy restriction which can fit various applications and the ASN.1 of EtriPolicyLanguage is [Figure 2]. The EtriPolicyLanguage has three fields. The period field is a start time and end time that a proxy can sign in a day. For instance, if notBefore 0900 and notAfter 1800, a proxy can sign only from at 9 AM to at 6 PM. The usage field indicates what kind of application a proxy can use. Examples of this field are e-commerce, bid, auction and so on. The target field point out servers which a proxy can access and the servers are described one of URL, DNS or IP address..



[Figure 3] Protocol for proxy certificate management

5. DELEGATION TRACE

The unforgeability and undeniability should be assured to use a proxy certificate. This chapter will show how these requirements are accomplished by using delegation trace.

In [Figure 3], P, called proxy, send a public key to I, called issuer, to request a proxy certificate. Before signing of the body which is the tbsCertificate, the I sends the body back to P to get P's agreement. And if the P agrees, the P sends the signature of the body to the I. Finally, the I creates the proxy certificate and return to the P.

When the P accesses the V, called verifier, the P sends a signed document with the proxy certificate. The V validates the proxy certificate and verifies the signature which the P signed the body to confirm that the P is designated proxy signer. And the V validates the proxy restrictions to authorize the P.

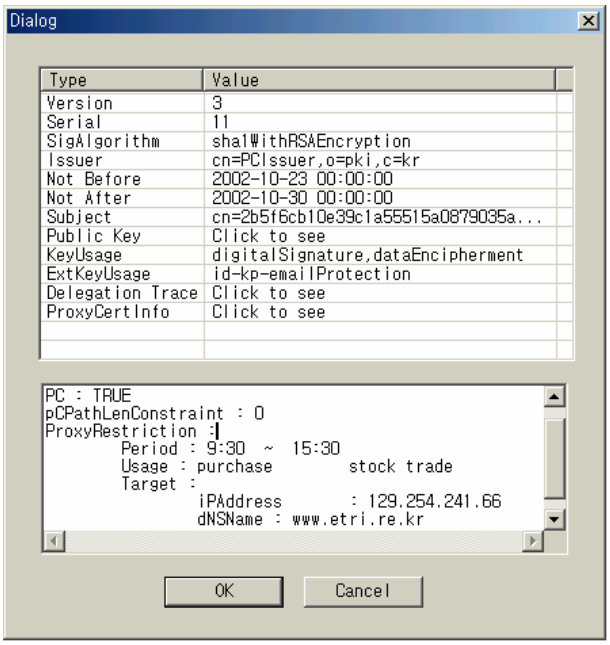
6. PROTOTYPE

This chapter describes the design and implementation of prototype to show how the proxy certificate can be used in an application. The prototype is implemented focusing to issuance of a proxy certificate, verification of a proxy signature, proxy restriction of a proxy certificate. The prototype consisted of proxy certificate issuer, proxy signer, and verifier. The Proxy issuer sets policies such as validity, issuer, key usage, and proxy restriction and it issues a proxy certificate and saves issued certificates to a database. A proxy signer requests a proxy certificate issuance, and manages issued certificates and its key pair which certificate is not issued yet, and makes signature with a proxy certificate. Verifier confirms a signature of a proxy certificate with issuer's certificate and validates proxy restriction in the proxy certificate. The prototype is examined for stock trade application. Figure 4 shows a proxy certificate that is issued according to a policy. The proxy certificate that is issued can only be used between 9:30 and 15:30, for purchase and stock trade, and in servers that are listed in Target field.

7. CONCLUSION

This paper described the proxy certificate that can be used to delegate the right of signature. We proposed a structure of proxy restriction and delegation trace protocol. We designed and implemented the prototype that shows proxy certificate issuance and verification.

In the future, a new restriction language should be developed. It should be flexible enough to specify policy of every application. Also, it should be interoperable to be used in heterogeneous systems. XML is a good candidate for the language. Finally, a proxy certificate technology should be applied real applications.



[Figure 4] Proxy certificate view

8. REFERENCES

[1] Housley, R., W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," Internet Draft draft-ietf-pkik-new-part1-12.txt (update to RFC 2459), January 2002.

[2] S. Tuecke, D. Engert, I. Foster, " Internet X.509 Public Key Infrastructure Proxy Certificate Profile" Internet Draft draft-ietf-pkix-proxy-02.txt, August 2002

[3] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature: Delegation of the power to sign messages", In IEICE Trans. Fundamentals, Vol. E79-A, No. 9, Sep., pages 1338-1353, 1996.

[4]Byoungcheon Lee, Heesun Kim, Kwangjo Kim, "Strong Proxy Signature and its Applications," Proceedings of SCIS2001, vol 2/2, pp.603-608, 2001