PKIX Working Group H. Kikuchi (Tokai Univ)
Internet Draft M. Sakurai (NEC)
H. Hattori (Meiji Univ)
Y. Sameshima (Hitachi Soft)
expires in six months March 1997

Internet Public Key Infrastructure:

Web-based Certificate and CRL Repository

Status of this Memo

Abstract

This document provides a specification how to publish and retrieve X.509 certificates and certificate revocation lists (CRLs). In the proposed method, the World Wide Web (WWW) is used for securely distributing certificates across a firewall in both human and machine readable syntax. A various certificate concerning information that includes certificates, CRLs, and certification authority (CA) policy are retrieved from an integrated single authority access point specified in X.509 version 3 extensions. The information access point accepts certification and revocation requests in the uniform access method based on the standard WWW.

1. Introduction

The first attempt for security enhancement of the Internet applications was electrinic mail. The Privacy Enhanced Mail (PEM) defined in [RFC-1421, 1422, 1423 and 1424] proposed X.509 public key certificates and hierarchically structured certification authorities (CAs), which are then adopted in MOSS [MOSS] and S/MIME [S/MIME]. These security protocols, however, require that a sender has to convey many certificates needed to certify its validity from a receiver because of the lack of certificates repository. Therefore, a big challenge to establish Public Key Infrastructure (PKI) is made by specifying profiles of the X.509 version 3 certificate and version 2 CRL [PKIX-1]. The PKI working group also proposed certificate management protocols in [PKIX-3], in which wide range of CA information format called PKI messages are defined by ASN.1 [ASN.1] that makes processing easier for management software, and simple socket based transport protocols.

However, in the practical point of view, the socket based transport protocol is problematic. First, most commercial organization have a firewall, which prevents intruder from gaining access to internal LAN and might reject PKI message transfer. For this reason, they shall provide a proxy service for each protocol. Second problem is confidentiality of PKI messages. Although most PKI message are public information, the initializing message such as certification or revocation requests require an extra capability of message encryption for achieving confidentiality. The third problem is the scaleability, which makes the service available in the wide scale networks. The requirement involves reducing traffic cost by a certificates cashing or a distributed database. The last problem is ASN.1 based definition which forces Basic Encoding Rule (BER) to transfer a PKI messages. For easier implementation, human readable encoding rule is appropriate.

To meet these requirements, this document defines World Wide Web (WWW) based certification and CRL repository. Since WWW is now one of the major application in the internet, almost all internet users can use it even if the site they belong has a firewall against intruders. The WWW provides some useful facilities for PKI; an information cashing by both a proxy server and client software, a secure transport layer service for confidentiality, a flexible request forwarding which can be used in CA and CA communication, and human readable and easier manipulating message format.

2. Basic Definition, Requirements and Assumptions

2.1 Overview

This document suppose simple restricted hierarchical certificate infrastructure rather than complicated CA web. Figure 1 shows an example of hierarchy of Publishing Authority (PAs), where PA2 has two subordinary PAs, PA1 and PA2, and PA1 has two users having certificate Cert1 and Cert2, respectively.

Every certificate has one information access point (IAP) from which any information with regards to users can be retrieved. The PA is responsible for all information it publishes. Thus, it also provides on-line validation service with and without CRLs. The PA certificate, which may be identical to the standard CA certificate, also has upper IAP entry. There is no different in IAP syntax among end entity, PA and CA. None of user and PAs publish certificate by theirselves, that is, subject information access extension is not necessary. The IAP specification is defined in Section 2.2.

The communication between entities was based on Hyper Text Transfer Protocol (HTTP) and its variation. The Hyper Text Markup Language is used as message format. Note that a subordinate entity is subject to be message sender and the higher entity just response to the requester. Thus, the coordinate entities never get direct communication with them. This assumption is convenient for conformance. The end entity and PA protocol is defined in Section 3.

```
                                                    +-----+
                                                    |     |
                                                PA3 V     |
                                             IAP3+---+    |
                                           +---->| *------+
                                   PA1     |     +---+
                              IAP1 +---+   |
                          +-------->| *-----+
               Cert1      |        +---+   |
                   +---+  |                |
                   | *----+                |
                   +---+  |        PA2     |
               Cert2      |        +---+   |
                   +---+  |        | *-----+
                   | *----+        +---+
                   +---+
```

Figure 1: Example of PAs hierarchy

2.2 Requirement for PKI Application

The PKI application needs certificates and CRL repository in the following three cases;

1. certificate retrieval.
   For example, a sender of secure message wants to retrieve the recipient's public key by which the message is to be encrypted.

2. certificate verification.
   The recipient of secure message check if the sender's certificate is not revoked by examining the corresponding CRL or asking the CA directly.

3. certificate and CRL publication.
   Soon after a certificate is issued by a CA, the new certificate shall be got access for anybody who wants it.

2.3 Requirement for X.509 Version 3 Certificate and Extensions

This proposal supposes that subset of X.509 Version 3 is used to form public key certificates. According to [PKIX1], the subject and issuer names in X.509 (v1) may be an empty sequence and subjectAltName and issuerAltName extensions (v3) shall be specified instead of the field. Even if the subject and issuer names are specified, the subjectAltName shall be given as an identification of certificate retrieval.

Most PKI applications require many kinds of information about certificate including policy information, CRL, and CA information. In [PKIX1], several access methods are defined for each kind of information. However, it is not so often case that a certain application has multiple access methods to PKI. Therefore, this document assumes that PKI application has an uniform access method of HTTP for for the simplification of PKI protocol.

As the same reason, the subjectInfoAccess, the authrotyInfoAccess and the caInfoAccess can be unified to the authorityInfoAccess. The subjectInfoAccess may be meaningless because a PKI user needs the information access point in two cases; (1) when it wants to verify the sender's certificate after it receives a secure message, or (2) when it wants to retrieve its recipient's certificate before it sends. In the first case, he/she cannot believe any information provided by the subjectInfoAccess, which the sender itself specify, and thus may be altered. Hence, he/she shall use the authrotyInfoAccess instead of the subjectInfoAccess. The other case,

he/she has not yet known the subject information access point which is to be specified the recipient's certificate, which shall be retrieved from any authrotyInfoAccess point she/he knows. Once PKI user gets the recipient's certificate, the subjectInfoAccess is no longer necessary for him/her. Consequently, the subjectInfoAccess is useless.

The AuthorityInfoAccess contains at least one AccessDescription in which the accessMethod and accessLocation shall specify httpID and appropriately URL that accepts "POST" method.

If this proposal is used, a standard certificate must specify

- authorityInfoAccess,

shall specify

- subjectAltName,
- issuerAltName,

may specify

- authorityKeyIdentifier,
- subjectKeyIdentifier,
- keyUsage,
- privateKeyUsagePeriod,
- certificagtePolicies,
- basicConstraints,
- nameConstraints,
- policyConstraints,

must not specify for avoiding confusion

- cRLDistributionPoints,
- policyMappings,
- subjectDirectoryAttributes,
- subjectInfoAccess,
- authorityInfoAccess,
- caInfoAccess.

2.4 Requirement for Publishing Authority

Since the number of PKI user increases step by step, the set of CAs always have to keep communicating with each other. Moreover, the number of CA also increases slightly, so, the hierarchical CAs structure is proposed in [RFC1422]. Where, the root CA is required to update all CAs and to manage the access path.

However, in practice, at the entrance to the Internet every organization has a firewall facility which restricts internet access to a particular application, service, and host in order for security consideration. Thus, generally, an CA runs within the firewall and only communicates with internal PKI users. Therefore, we need a publishing authority (PA) that is set up for each CA and works as a certificate repository outside of the firewall. Figure 2 shows this structure.

The transaction between particular entities can be easily restricted by a firewall, thus, it does not spoil the security of CA. An internal static information access point provides a simple and uniform access method for PKI users. Any information stored in external PA is not secret information and may be different to that of internal PA.

```
                                           [root PA]
                            The Internet       |
                           ---+------+---------+-
                              |      |
                         |    |      |   |
                   [CA]--+---[PA]  [PA]--+--[CA]
                   /|    |               |    |
             PKI users   |               |   PKI users
                        firewall    firewall
```

Figure 2. Relationship between PA and CA

3. Transport Protocol

3.1 Information Access

Information access point (IAP) is specified by the subjectInfoAccess field in certificate extension. The IAP is a point from which certificates are distributed and on-line verification service is provided.

The PA server can be implemented as a standard HTTP server which enables CGI facility. The IAP server works as PA, CRL distribution point, policy repository, verification server, and certificate repository. The PA server management certificates in a specific closed organization, and communicates with upper PA server which knows the all subordinate PA server's location.

A PKI application points at least one IAP so as to retrieve locations of other IAPs.

An information transfer is based on HTTP with method POST. Thus, the typical query is formated as follows;

```
        POST IAP/queryType HTTP/1.0
        name1=value1&name2=value2&...&namen=valuen
```

where "queryType" is a type of query and a pair of "name" and "value" are used to send PKI message. All fields are subject to be formed in standard encoding rule defined in [HTTP].

```
        HTTP/1.0 200 OK
        Date: Wednesday
        MIME-version: 1.0
        Content-type: text/html

        <HEAD><TITLE>queryType</TITLE></HEAD>
        <BODY>
        <H3> statusCode </H3>
        <H1> statusMessage </H1>
             information
        </BODY>
```

Where, "queryType" is the same as the type given in sending request. The "statusCode" contains a status with three digit codes. With at least one space, the "statusMessage" and "information" are interpreted in corresponding semantics. The syntax of "information" depends on the query type, and will be defined section 5.

3.2 Type of Query

This document defines the followings query types.

1. certreq
2. revokereq
3. lookupreq
4. verifyreq

3.2.1 Initial Registration type "certreq"

Type "certreq" is used for sending certification request to CA. This query may be used only if the PA works as CA or has some means to relay the request to the corresponding CA. The certreq request shall be sent with some of the following pairs of name and value.

name	value
o	Organization
ou1	Organizational unit

ou2	Organizational unit 2
ou3	Organizational unit 3
ou4	Organizational unit 4
cn	Common name
n	public component of RSA cryptosystem
email	RFC822 style email address
info	URL of user's home page
key	public key encoded in corresponding BER
acct	User identification
pass	User password
loginname	Manager identification
password	Manager password

The pair "o", "cn", "n", "email" are critical pairs. The name "n" implicitly identifies a modulo value when public component of 0x10001 is used in RSA cryptosystem. Otherwise, name "key" shall be used to convey public key information which is encoded in the corresponding BER rule. Either of "n" and "key" must be given. The "acct" and "pass" may be used for user authentication. If these pairs are missing, the response shall contain the other pairs as hidden attribute   and be used as confirmation of user information. Alternatively, the "loginname" and "password" may be used by the CA manage.

The response consists of statusCode, statusMessage and information.

statusCode	statusMessage	information
200	"accept your request"	the issued certificate encoded in Base64 encoding rule.
301	"incomplete request"	the missing pair and the other information
302	"duplicate request"	the certificate has already been issued.
303	"reject your request"	any other reason why the request failed.
304	"service not available"	the PA does not accept this request.

3.2.2 Certificate Revocation "revokereq"

The "revokereq" is a request to revoke a certificate. To prevent malicious PKI user from revoking other's certificate, this request should be sent with a proof of possession of the secret key. The simplest way is to use conventical application that supports digital signature.

name	value

sig	digitally signed revocation message

statusCode	statusMessage	information
200	"accept your request"	nothing (the certificate is revoked)
301	"invalid signature"	nothing
302	"duplicate request"	nothing (the certificate has already been revoked)
303	"reject your request"	any other reason why the request failed.
304	"service not available"	the PA does not accept this request.

3.2.3 Certificate Distribution "lookupreq"

The "lookupreq" type is used for retrieving and searching certificate, CRLs, and any other information. The PA server may forward a request to other PA server when it does not has sufficient information to response to the request.

Certificate is identified by either of the following names;

a. email address   b. Distinguished Name

Both identifiers must be fully specified because a substring matching rule might violate a privacy issue when the PA is the outside of firewall. The lookup query is sent with the following pairs of names and value.

name	value
o	Organization
ou1	Organizational unit
ou2	Organizational unit 2
ou3	Organizational unit 3
ou4	Organizational unit 4
cn	Common name
dn	subject/CA Distinguished Name.
email	subject/CA email address
object	"policy" (policy description and mapping) "cert" (CA or subject certificate) "crl" (CA CRL)

The pairs of "o", "ou1", "ou2", "ou3", "ou4", and "cn" specify intend distinguished name. Alternatively, the "dn" pair may be used to specify distinguished names. When the specification is incomplete, the PA may reject it for privacy issue or accept it as substring matching. Whether the request is for subject or for CA can be

identified by the distinguished name. For example, a distinguished name containing "cn=Authority" is a request for CA, otherwise for subject. The "object" specifies what information is required and takes "cert" in default. For instance, a request with "object=crl" is equivalent to the request by crlDistributionPoint extension.

The response consists of statusCode, statusMessage and information.

statusCode	statusMessage	information
200	"accept your request"	the certificate, policy or CRL encoded in Base64 encoding rule.
301	"revoked"	the reason of revoked
302	"reject your request"	the reason why the request failed.
303	"service not available"	the PA does not accept this request.

3.2.4 Certificate Verification "verifyreq"

Type "verifyreq" is used for validation check of certificate. This document does not support path validation. The verifyreq request shall be sent with the following pairs of name and value.

name	value
cert	certificate embedded in CGI coding rule
certsig	certificate embedded in CGI coding rule
crl	DN of intended certificate
sn	serial number of a certificate
time	GENERALIZED TIME when certificate should be checked to be valid.
dn	request originator's distinguished name

The "certsig" request has the PA digitally signed its response. The PKI user specify a certificate by either sending the whole certificate with "cert" or just sending "sn" when the implicit PA server can be determined. The "time" is optional pair, which means when the certificate to be examined. This option is used when one wants to verify if an old message was valid at that time.

When "cert" is specified, the certificate to be verified is embedded into the value in CGI coding rule. The "certsig" is same as the "cert" except but it responses with message integrity check code.

When "crl" is specified, PA server only make sure if the intended certificate is already revoked.

The "dn" is used when the PA provides verification service only to restricted users.

The response of "cert" request is as follows.

statusCode	statusMessage	information
200	"valid"	nothing (the certificate is valid)
201	"not revoked"	nothing (the certificate is not revoked)
301	"revoked"	the reason of revoked
302	"hold"	the reason of hold
303	"reject your request"	any other reason why the request failed.
304	"service not avialable"	the PA does not accept this request.

Some example of reason of revoked are such that the key was compromised, or the affiliation was changed.

3.3 Correspondence to preceding PKI draft

This document corresponds to PKI management protocol defined in [PKIX3]. Table 1 shows the correspondence and side effect occurred by a request.

Table 1. Correspondence of methods

PKI method	PA method	Side effect
certStatus	verify	no
certRetrieval	lookup	no
caPolicy	lookup	no
caCert	lookup	no
CRLDistributionPoint	lookup	no
certReq	certreq	yes
revokeReq	revokereq	yes

3.4 Inter-PA Protocol

If a request to a PA concerns information not stored in the PA, the PA shall manage to obtain it by relying the request to an appropriate PA. This section define an inter-PA transaction.

3.4.1 PA Model

Suppose that there are PA1, PA2 and RootPA, and PA1 has a request for retrieving information from PA2. The PA1 and PA2 does not have their locations but the access point to RootCA. There are two possibilities for PA1 to get access to PA2 (Figure 3).

- Model 1. [referral] PA1 sends the request to Root PA (1), which then   replies to PA1 with the access point to PA2 (2). PA1 sends it to PA2 again (3), and finally PA1 gets the information from PA2.

- Model 2. [chaining] PA1 sends the request to Root PA (1), which redirects it to PA2 on behalf of PA1 (2). PA2 answers to Root PA (3), which forwards it to PA1 (4).

```
              +---->[RootPA]                          +---->[RootPA](2)---+
              | +---(2)                               | +---(4)     <---+ |
              | |PA2                                  | |               | |
              | |                                     | |               | |
           (1)| V                                  (1)| V            (3)| V
             [PA1] (3)-----------> [PA2]             [PA1]             [PA2]
                   <-----------(4)

                   Referral                                Chaining

                           Figure 3. Inter-PA models
```

3.4.2 Referral Model

To redirect a request to another PA server, the root PA responds to the requester with the following HTTP redirect message consisting HTTP header and HTTP body.

```
HTTP/1.0 302 Found
Date: Monday, 20-Jan-97 13:33:29 GMT
Server: NCSA/1.1
MIME-version: 1.0
Location: http://xxx.yy:zz/method
Content-type: text/html

<HEAD><TITLE>Document moved</TITLE></HEAD>
<BODY><H1>Document moved</H1>
This document has moved <A HREF="http://xxx.yy:zz">here</A>.<P>
</BODY>
```

Where the URL "http://xxx.yy:zz/method" specified by the Location HTTP header   provides information where the query to be sent next. This is a control message used in the standard HTTP transaction [HTTP].

The root PA must respond with either correct PA location or error message to mean that there is no certificate. To do this, all correspondences between identifiers and IAP locations should be notified by the root PA.

In this model, PKI application or PA must support HTTP redirect message. Each round trip time is short, but PA has to send the same query to several servers.

3.4.3 CGI Chaining Model

To implement CGI chaining model, the CGI script in root PA produces an extra CGI message before it responds to the request originator.

The request originator, PA1 or PKI application, does not have to send request many times, but have to wait longer time than that of referral model. According to [Mine], the estimated total round trip time is less than that of the referral model. Since PA communicates with a particular PA, the access control at firewall can be easily set up.

4. Security Consideration

4.1 Confidentiality of transaction

To prevent message from being eavesdropped, secure communication channel such as SSL shall be used. Especially, initial registration process is critical to eavesdropping. Since user authentication is checked by "uid" and "passwd", a client software is not required to have its own certificate. Under the assumption, PKI message protection proposed in [PKIX3] need not here.

4.2 Non-Repudiation

The verify request supports the time to be checked and digitally signed response. This can avoid a message sender from denying the message. To enable this service, any PA must manage all certificates which it has already issued, including revoked certificates.

4.3 Privacy

In the lookup request, the support of substring matching facility may distribute private information to outsiders, and thereby may be used for sending an advertisement via email.

5. ASN.1 encoding rule in HTML

5.1 Definition

A certificate management protocol is defined in ASN.1 syntax in [PKIX3]. The BER is not human readable but is better for security enhancements such as an integrity checking, whereas the ASCII text is human readable but not suitable for machine processing. Therefore, this document defines ASN.1 encoding rule in HTML, which can be both human and machine readable encoding.

In the BER, any data type is formed with three elements, tag, length, and value. Instead of the length field, the HTML encoding identifies the value field by specifying the data start tag and the data end tag. The printable string data type and UTC time type are specified by the <H3> and </H3> tag. The other data type is defined by the <H5> and </H5> tag. The structured types, SET and SEQUENCE, are defined by the <UL> tag and <OL> tag, respectively. For the inverse function of the encoding, the corresponding data tag number follows the tag name in two octet hexadecimal numbers.

The printable string data value is represented in ASCII. The other data value is represented in hexadecimal octet string. The document does not define a means to encode bit string data. For easier implementation, this document define a set of data value encoded in Base64, which is identified by <Blockquote> and </Blockquote> tag. This notation is useful when PKI application transfers the whole certificate without interpreting the contents.

The encoding rule allows no optional notation, no tagged type and no default value. Every data type is specified explicitly in order to for uniquely distinguishing data types.

Table 2 shows main data type and the encoding format. Where, "n", "s" are examples of numbers and string, and "a" and "b" are of any ASN.1 data type. For example, an integer 12 is coded by "<H5 03>0C</H5>".

Table 2. HTML Encoding Rule

ASN.1 Data Type	HTML Encoding

BOOLEAN	<H5 01> n </H5>
INTEGER	<H5 02> n </H5>
BIT STRING	<H5 03> n </H5>
OCTET STRING	<H5 04> n </H5>
NULL	<H5 05> </H5>
OBJECT IDENTIFIER	<H5 06> n </H5>
PrintableString	<H3 13> s </H3>
IA5String	<H3 16> s </H3>
UTCTime	<H3 17> s </H3>
GeneralizedTime	<H3 18> s </H3>
SEQUENCE {a, b}	<OL 30> <LI> a <LI> b </OL>
SET {a, b}	<UL 31> <LI> a <LI> b </UL>
xxx (Base64 format)	<BlockQuote> xxx </BlockQuote>

5.2 Example

A PKI message format and the corresponding encoding are as follows. Note that the tagged data protection and extraCerts are not omitted.

```
    PKIMessage ::= SEQUENCE {
      header           PKIHeader,
      body             PKIBody,
      protection   [0] PKIProtection OPTIONAL,
      extraCerts   [1] SEQUENCE OF Certificate OPTIONAL
    }

    <OL 30>
      <LI> PKIHeader
      <LI> PKIBody
      <LI> PKIProtection
      <LI> <OL 30>
                <LI> Certificate 1
                <LI> Certificate 2
           </OL>
    </OL>
```

A distinguished name consisting of countryName="JP", organizationName="ICAT", and organizationalUnitName="Certification Authority" is encoded as follows.

```
    <OL 30><LI>
         <UL 31><LI>
            <OL 30><LI>
               <H5 06>550406</H5><LI>
               <H3 13>JP</H3>
```

```
               </OL>
            </UL><LI>
            <UL 31><LI>
               <OL 30><LI>
                  <H5 06>55040a</H5><LI>
                  <H3 13>ICAT</H3>
               </OL>
            </UL><LI>
            <UL 31><LI>
               <OL 30><LI>
                  <H5 06>55040b</H5><LI>
                  <H3 13>Certification Authority</H3>
               </OL>
            </UL>
         </OL>
```

Acknowledgement

The authors thank Mr. Ohbayashi, Mr. Kobayashi, Mr. Kuroda, Mr. Fujimoto, and Mr. Wada for their comments to this proposal. The authors also thank the other researchers joining the Initiative Computer Authentication Technology (ICAT), and the Interauth working group of WIDE project.

Reference

[PKIX-1] R. Housley, et. al., "Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile," <draft-ietf-pkix-ipki-part1-03.txt>, December 1996

[PKIX-3] S. Farrell and C. Adams, "Internet Public Key Infrastructure Part III: Certificate Management Protocols," <draft-ietf-pkix-ipki3cmp-02.txt>, December 1996

[RFC1422] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management," RFC 1422, February 1993.

[S/MIME] S. Dusse, "S/MIME Message Specification: PKCS Security Services for MIME", <draft-dusse-mime-msg-spec-00.txt> September 1996

[MOSS] S. Crocker, et. al., MIME Object Security Services, RFC 1848, October 1995

[HTTP] T. Berners-Lee, R. Fielding, H. Nielsen, "Hypertext Transfer

Protocol -- HTTP/1.0", RFC 1945, May 1996

[ASN.1] B. Kaliski, "A Layman's Guide to a Subset of ASN.1, BER, and DER", ftp://ftp.rsa.com (layman.ps), June 1991

[Mine] M. Sakurai, et.al., A Design of Certificate or CRL Distribution Architecture between Certification Authorities, The 1997 Symp. on Cryptography and Information Security (SCIS'97), 8D, January 1997

Security Considerations

This entire memo is about security mechanisms.

Author Addresses:

Hiroaki Kikuchi
Dept. of Electrical Engineering
Tokai University
1117 Kitakaname, Hiratsuka, Kanagawa 259-12, Japan
kikn@ep.u-tokai.ac.jp

Mine Sakurai
NEC Corporation
garashi bldg., 2-11-5 Shibaura, Minato-ku, Tokyo 108, Japan
m-sakura@ccs.mt.nec.co.jp

Hiroyuki Hattori
Meiji University
1-1-1, Higashi-mita, Tama-ku, Kawasaki, Kanagawa 214, Japan
hhat@isc.meiji.ac.jp

Yoshiki Sameshima
Hitachi Software Engineering Co., Ltd.
6-81 Onoe-cho Naka-ku, Yokohama, Kanagawa 231, Japan
same@ori.hitachi-sk.co.jp