Real-time Certificate Status Validation Model With CSIPrvider

JIN KWAK*, KYUNG-JIN KIM*, SOO-HYUN OH*, DONG-HO WON*
HYUNG-KYU YANG**

*Information & Communication Security Laboratory
Sungkyunkwan University
300 Chunchun-Dong, Jangan-Gu, Suwon, Kyunggi-Do
KOREA
{jkwak, kjkim, shoh, dhwon}@dosan.skku.ac.kr

**College of Science and Engineering
Kangnam University
2 Gugal-Li, Gihung-eup, Yongin, Kyunggi-Do
KOREA
hkyang@kangnam.ac.kr

Abstract: The certificate using services to validate the public key are increasing according to the spread of the public key infrastructure application. To verify the certificate, the client must confirm the availability of certificate’s current status first. Various methods to validate the certificate have been proposed so far and most of them are CRL-based. But those CRL-based methods have many problems because of the CRL’s periodicity. Therefore, the CA in the field that requires frequent modification needs to provide the latest CSI(Certificate Status Information) to the client in a real-time. In this paper, we analyze the requirements of service objects and propose a new model which can offer the timely CSI to the client in a real-time.

Key-Words: PKI, CSI(Certificate Status Information), Real-time, Timeliness

1 Introduction
With the rapid progress of research to construct a secure network, a lot of new services have been offered. Those services are expanded with the adaptation of public key infrastructure that provides entity authentication, data integrity and non-repudiation about the transaction. These certificate using services with public key infrastructure are mostly used for an entity authentication. The certificate must be validated before verifying it and the CSI is important in the fields that use lots of certificates [1][2].

CRL, Delta-CRL and Over-Issued CRL are the typical method to verify the availability of certificate. But the CRL-based certificate verification method cannot provide the current CSI [3]. OCSP has been proposed to overcome this problem. But it also cannot be used in the field that requires a real-time CSI.

In this paper, we analyze the requirements of CA, validation information providing server, and clients then propose a real-time Certificate Status Validation Model(RCSV) with the Certificate Status Information Provider(CSIPrvider). This paper is consisted as follows. In section 2, we analyze the problems of verification process and define the terminology and related work. In section 3, we analyze the requirements of each objects that consist the certificate validation service. In section 4, we explain the RCSV model, a new protocol with CSIPrvider and operation of proposed model. Finally, in section 5, we bring to a conclusion of this paper.

2 Definition & Related Work
In this section, we define the terminology used in the proposed RCSV model and examine the problems of existing certificate status verification methods.

2.1 Terminology
The terminologies used in this paper are as follows:

- **Real-time**: means that the definite transmission and response time is guaranteed. When CA produces a Certificate Status Information(CSI) and offers it to the RCSV Server, CA can guarantee a definite transmission time and the RCSV Server can also guarantee a definite response time for the client’s request.

- **Timeliness**: The response to the client’s CSI request must be the timely. If the CSI is issued periodically, it cannot provide the latest information of certificate status to the client.

- **CSIPrvider**: is a transmission module of the latest CSI between CA and RCSV Server.
**RCSV Server**: receives information of modified certificate status from CA and provides server to client. It is a responder of the service.

**RCSV Client**: is a user of the service proposed in this paper. The user can be both the verifier of certificate and the requestor of service.

**Certificate Status Information (CSI)**: is information about availability of each certificate. It is the information of each revoked certificate status.

**Certificate Information Transmission Protocol**: is a protocol to provide the CSI to RCSV Server from CA. It is called CITP.

**Validation of Certificate Availability**: is a little bit different from verification of the certificate. It contained integrity of certificate and verification of validity period.

### 2.2 Related Work

In this subsection, we examine the existing certificate status verification methods. CRL is standardized and most widely used method. In this paper, we explain about the CRL-based certificate status verification method.

#### 2.2.1 CRL (Certificate Revocation List)

Certificate Revocation List (CRL) is the most widely used method to validate the certificate's status. The CA signs to the certificate including the serial number and reason of expire and make it public. Then the client downloads the CRL and searches for obtaining the CSI information[2].

CRL contains a serial number and reason of all revoked certificates. It is the general method to show the revoked reason. But it can't give the current status because it is issued periodically and it has a communication overload because of download whole CRL [4][5].

#### 2.2.2 Delta-CRL

Delta-CRL is developed to improve periodical problem and communication overload. This method doesn't contain the whole CRL and only contains the modified list from recent to new CRL. The communication overload is decreased because of it's small size and the certificate status is provided in a proper time. But it should be issued together with the whole CRL [2][4][5].

### 2.2.3 Over-Issued CRL

Over-Issued CRL is a method to notify the CRL that is overlapping the term of validation and different expire time. There are several CRLs valid on a specific time, so the client's process of obtaining the CRL from the CA is dispersed. Therefore, CA can reduce the communication overload. This method also can be applied to the Delta-CRL [4][5].

#### 2.2.4 Indirect CRL

The CA that issues the certificate also issues the CRL. But, in indirect CRL, other CA that doesn't issue the certificate issues the CRL. One certificate can contain several CSI from other CAs. In this method, a client doesn't have to bring the CRL from the exact CA that issue the certificate. So s/he can reduce the communication overload. In this method, trusted third party is needed [4][5].

#### 2.2.5 OCSP (Online Certificate Status Protocol)

OCSP is proposed to provide the current certificate status information. It is composed of client and server, and standardized as IETF RFC2560. This is a protocol that provides CSI to a client without using CRL and it is used online between the server and the client. If a client connects to a server and requests a CSI that s/he need, the server searches that information and digitally signs it [3][6][7]. Then the server sends it to the client. The client can obtain the CSI using the OCSP. But it does not contain any concrete explanation about the operation and only defines the format and structure of a message between the server and the client.

### 3 Requirement of Components

As mentioned before, OCSP can provide a CSI to a client, but it is not used in practice because there is no concrete definition of its operation and also the history is short. To make use of OCSP system in practice, the request/response between the CA and the server, the server and the client must be accomplished in a real-time. And the response must contain the latest CSI [3][6][8].

#### 3.1 CA (Certification Authority)

The requirement of CA is as follows:
(1) Independence of CA

The main purpose of CA is issuing and managing the certificate. Therefore, this should not be affected by the separate RCSV Server. And CA must be constructed independent of RCSV system related work.

(2) Ability of Information Storage

In the case that the CA and RCSV Server shares the database, important information in addition to the CSI could be exposed to an external hazard. Because it needs an additional thorough access control, we will not consider it in this paper.

(3) Reduction of Overload

The CA has to reduce the unnecessary communication overload by providing only the certificate information that RCSV Server takes charge of.

(4) Provides of Additional Information

The CA has to issue the certificate with an additional RCSV Server's location so that user may use the service and also provides an access method to the RCSV Server and the URL.

3.2 RCSV Server(Real-time Certificate Status Validation Server)

The requirements of the RCSV Server are as follows:

(1) Ability of Message Process

RCSV Server should be able to take care of client's request message and generate a response message to that request.

(2) Providing Real-time Response

After the RCSV Server generates the response message, it should able to send the response message to the client in a real-time. We define the meaning of real-time in section 2.

(3) Ability of Searching Information

The method that uses a general Database and File system can overload the system and delay the service. Therefore, RCSV Server should be able to search and extract the CSI using Main Memory Database.

(4) Receipt of Real-time CSI

The RCSV Server needs a protocol that can synchronize the CSI in a real-time to receive and process the CSI from the CA.

(5) Decentralization of Service Request

If requests of certificate validation are excessively concentrated to the RCSV Server, it is possible to fall into the denial of service state. So the RCSV Server should be able to decentralize the requests to other RCSV Servers.

3.3 RCSV Client(Real-time Certificate Status Validation Client)

The requirements of the RCSV Client are as follows:

(1) Ability of Message Process

The RCSV Client should be able to take care of RCSV Server's response message and generate the request message. And it should be able to process the extensions field, too.

(2) Timeliness of CSI

The CSI that RCSV Client acquires should contain the latest CSI at the time of the client's request.

(3) Guarantee of Definite Response Time

The definite response time for the RCSV client's request could be guaranteed by the RCSV Server. And the service should not be delayed.

(4) Lightness of CSI

The length of the RCSV Client acquired CSI must be minimized. So it doesn't overload communication overload both RCSV Server and Client.

The current CSI is very important to client using the certificate. Therefore it must be constructive of continuous service, if such service stopped for a while and cannot provide service worried over serious damage of client.
4 Real-time Certificate Status Validation Model With CSIProvider

In this section, we propose a Real-time Certificate Status Validation Model with CSIProvider that provides the timely CSI in a real-time.

4.1 Motivation

The PKI provides confidence, safety and security of information. From this, the user can use the online service in safety.

On the area using PKI, the current status of certificate is important. So the availability of the certificate must be confirmed before using the service. To validate the certificate, CA issues revoked list, but the CRL-based method isn’t suitable for the field that requires the CSI at the exact point of time because of periodicity. Also, the existing on-line certificate validation model obtains the modified information of the public key certificate and provides current CSI. Because of this, it can provide the CSI to the client but is not sufficient to provide timely CSI in real-time. In this paper, we propose a RCSV model that can provide a current CSI in real-time.

4.2 Architecture of RCSV Model

The proposed RCSV model is made up CA, CA database, CSIProvider protocol that sends information between CSIProvider and RCSV Server, database of RCSV Server and a User. Fig.1 shows the RCSV model.

- Issuing and managing the whole CRLs for the revoked certificate.
- Issuing and keeping the new modified status information of certificate.
- When there is any modification of the certificate, CA informs it to the CSIProvider.
- CSI may include the certificate’s serial number, distinguished name(DN), revoked reason and etc.

①CA’s Database(DB1)
- The whole CRLs created and issued by CA is stored in CA's database(DB1)
- Storing and updating the newest information of certificate status.

②CSIProvider
- CSIProvider is a transmission module that provides new CSI from CA to RCSV Server.
- It receives modified CSI that is created in CA, then transmits it to the RCSV Server at once.
- It transmits the same CSI that is stored in CA’s database to the RCSV Server.

③CITP
- CITP is a mutual agreement protocol between the CSIProvider and the RCSV Server.
- It cannot delete or insert any information issued by the CA and only can transmits the information to the RCSV Server.
- It must provide data integrity and security.
- It must guarantee real-time property as definite response time.

④RCSV Server
- RCSV Server stores the latest CSI to it’s own database(DB2).
- RCSV Server checks the CSI in DB2 and provides it to the client.
- If the service request is excessively concentrated on the RCSV Server, it is possible to run into state of denial of service. Then the RCSV Server can request to disperse the requests to other RCSV Servers.

⑤RCSV Server Database(DB2)
- It only have the modified CSI, not the whole CRL.
- It has the same CSI issued by the CA and stored in DB1.
4.3 CITP, RCSV Request and Response
In this subsection, we define the CSI transmission protocol created by CA, and the formats of request and response message.

4.3.1 CITP(Certificate Information Transmission Protocol)
CITP is a new transmission protocol that provides the latest CSI from the CSIProvider to the RCSV Server. It receives the newest CSI created in CA, then transmits it to the RCSV Server at once. It can't delete or insert any information.

It is the module that can transmit the newest CSI to the RCSV Server. Model of the certificate validation using CSIProvider provides the latest CSI to the client in real-time using a new protocol called CITP.

The ASN.1 definition of the CITP and the meaning of each fields of the protocol are described as follows [9][10].

CertStatusMessage field is composed of header, body and signatureValue.

CertStatusMessage ::= SEQUENCE { 
    header    CertStatusHeader
    body      CertStatusBody
    signatureValue BIT STRING OPTIONAL }

CertStatusHeader field is an explanation of the sender and recipient about CSI generated by the CA. The header is composed of a sender and a recipient. The sender is a CA and the recipient is a RCSV Server.

CertStatusHeader ::= SEQUENCE { 
    Sender    GeneralName
    Recipient GeneralName }

CertStatusBody field provides substantial CSI. This field is composed of certStatus that presents the status of each certificates and the certStatusInfo that presents the additional information of each certificates.

CertStatusBody ::= SEQUENCE { 
    certStatus CertStatus
    certStatusInfo CertStatusInformation }

CertStatusInformation field is composed of serial-number that indicates each certificate’s serial number, RevokedReason that indicates the revoked reason, Time that indicates the revoked time, and the CRL Location that supports the searching for the CRL.

CertStatusInformation ::= SEQUENCE { 
    certSerial INTEGER 
    reason RevokedReason
    revocationTime Time
    location CRL Location OPTIONAL }

4.3.2 RCSV Request
RCSV Request message is the message that client, who using the service, requests the CSI to the RCSV Server. This message sends the CSI to the server including signature of requestor, so availability of the certificate is held back before receiving the RCSV Response of the RCSV Server.

The ASN.1 definition of the CITP and the meaning of each fields of the protocol are described as follows.

RCSVRequest ::= SEQUENCE { 
    version INTEGER DEFAULT 0 
    requesterName GeneralName
    requestCertList SEQUENCE OF 
        RequestCertList
    requestExtensions EXPLICIT Extensions 
        OPTIONAL }

signature OPTIONAL Signature }

version specifies the version of the message and it’s initial value is DEFAULT 0. requesterName is the general name of a requestor. requestCertList field is the information of specifies the certificates in the request. requestExtensions field indicates beforehand mutual agreement between RCSV Server and Client and this field is used to request an additional information.

RequestCertList ::= CHOICE { 
    CertID CertID
    IssuerSerial [0] IssuerSerialNumber
    PkCert [1] Certificate
    CertHash [2] OCTET STRING }

CertID ::= SEQUENCE { 
    hashAlgorithm AlgorithmIdentifier
    issuerNameHash OCTET STRING 
        -- Hash of issuer’s DN
    issuerKeyHash Certificate 
        -- Hash of issuer’s Public key
    certSerialNumber CertificateSerialNumber }
CertID field is composed of hash algorithm OID, hash value, and a serial number of the certificates. hashAlgorithm is used to hash the issuer’s DN and public key. certSerialNumber contains the requested serial number of certificate. issuerSerial indicates the proper number of issuers, and pKCert indicates the public key certificate.

Signature ::= SEQUENCE {
  signatureAlgorithm AlgorithmIdentifier
  signature BIT STRING
  certs EXPPLICIT SEQUENCE
              OF Certificate OPTIONAL }

Signature field is composed of signatureAlgorithm used to make a signature and signature that represents the BIT STRING

Signed request message shall identify the requestor in the requesterName field of RCSVRequest. Signed request message may include in the certs field of Signature element certificate that assist the RCSV Server to verify the requestor’s signature.

4.3.3 RCSV Response

RCSV Response is the response message that includes certificate validation result. It is done by the RCSV Server that receives the request message from the client. Response message sent to the client also contains the responder’s signature. RCSV Server checks the status of certificate and provides it to the client.

The ASN.1 definition of the RCSV Response message is given in below, and the meaning of each field of the message is described as follows.

RCSVResponse ::= SEQUENCE { signedSet SET {
  version INTEGER DEFAULT 0
  responderName GeneralName
  certValidationResult CertValidationResult
  response SEQUENCE OF ResponseData
  responseExtensions EXPPLICIT Extensions
              OPTIONAL }
  signature OPTIONAL Signature }

version is specifies the version of the message, initial value is DEFAULT 0. responderName is the general name of responder. certValidationResult field is the result of specifies the certificates for the client’s request. responseExtensions field indicates that beforehand mutual agreement between RCSV Server and Client, this field used response about additional information. signature is signature of RSCV Server. CertValidationResult field is the construction based on certStatus in CITP and contained as follows.

CertValidationResult ::= ENUMERATED {
  valid (0)
  internalError (1)
  finished (2)
  revoked (3)
  tryLater (4)
  unauthorized (5)
}

valid indicates the validity of certificate. internalError indicates the server reached inconsistent internal state. finished indicates that the certificate is not valid any more. revoked indicates that the certificate is revoked before the term of validity because of the revoked reason. tryLater indicates that the server is running but returns a status for the requested certificate. So it is used to indicate that the service exists, but it is temporarily unable to respond. unauthorized is the client who is not authorized to the server.

ResponseData field includes an additional information of response message and is based on the certStatusInformation of CITP.

ResponseData ::= SEQUENCE {
  responderID ResponderID
  producedAt GeneralizedTime
  reason RevokedReason
  revocationTime Time
  location CRL Location OPTIONAL
  responseExtensions EXPICIENT Extensions
              OPTIONAL }

ResponderID indicates the identifier of the responder. producedAt indicates the time at which the responder signed the response. RevokedReason indicates the reason of revoked certificate. Time is the time of certificate revocation. CRL Location gives support to refer to CRL.

All the above information is digitally signed with the private key of the RCSV Server, and the signature can be verified the public key contained in the public key certificate issued by the CA.

4.4 Operation of RCSV Model
The architecture of the Real-time Certificate Status Validation Model With CSIPrivate Provider that proposed in this paper is showed figure 2. Service is provided by this sequence and operation in the fig.2.

**Fig. 2 Operation of RCSV**

1. **Generation of new CSI**

   The CA generates the user information, certificate, CSI and CRL and stores them in its own database (DB1). The CSI contains the latest information of certificate such as the revocation or the modification of the certificate. Then the CA stores it to DB1 and sends it to CSIPrivate Provider at the same time after the generation of new CSI. The new CSI contains the certificate’s serial number, DN, current status and the reason of modification/revocation.

2. **Transmission of the CSI**

   After receiving the new CSI from the CA, CSIPrivate Provider sends it to the RCSV Server instantly. CSIPrivate Provider uses the CTPP negotiated between the CSIPrivate Provider and the RCSV Server and the CTPP provides the reliability of the information. The CSIPrivate Provider only can transmit the CSI to the RCSV Server and cannot add/delete any information to the CSI issued by CA.

3. **CSI storing of the RCSV Server**

   RCSV Server stores the new CSI to its own database (DB2) after the validation. The CSI transmitted from the CSIPrivate Provider only contains the modified information and it does not contains the whole CRL.

4. **Request of the certificate validation**

   The user can validate the certificate by requesting the certificate information that s/he wants to validate to the RCSV Server and validating the replying message from the RCSV Server. The request message only contains the requested information, there is less communication overload.

5. **Search/extraction of the certificate status**

   If the RCSV Server receives the request message from the user, it searches the CSI stored in DB2. Because the CSI in DB2 is equivalent to the latest CSI issued by CA, it can provide the timely certificates validation information to the client.

6. **Response of the certificate validation result**

   RCSV Server provides the result of reference to the client with the format of RCSB Response. Response message contains the information that can present the current certificate status. Response message can provide not only the certificate status but also the revocation reason, revoked time and the location of CRL in the case of client’s request. RCSV Response provides the real-time property. Because the proposed model obtains the latest CSI using the CTPP, it can provide the timely CSI to the client.

### 4.5 Characteristics

The proposed model provides CSI to the client in real-time by using the CSIPrivate Provider. By defining the new protocol, the model can transmit the new information in real-time and provide the timeliness of CSI without any overload.

#### 4.5.1 Timeliness of CSI

Unlike the CRL based models, the proposed model can send the modified information to the RCSV Server instantly. So it can provide the timely response to the client.

#### 4.5.2 Real-time property of Certificate Status Information and RCSV Response

The modified CSI issued by the CA is transmitted to the RCSV Server through the CSIPrivate Provider instantly. The response time to the client’s request can be guaranteed in the proposed model by searching the information in the RCSV Server. So the proposed model can respond to the client in real-time.
4.5.3 Lightness of Certificate Information
The proposed model minimizes the length of the CSI provided to the client by the CA and the RCSV Server. So it can provide CSI without overloading the client and the CA.

4.5.4 Decentralization of RCSV Request
If there are several requests at the same time, it is possible that the Response Server cannot provide the service. But the proposed model can provide the service by dispersing the request messages of the clients with several RCSV Server.

4.5.5 Selectivity of Certificate Information
The client requests the specific certificate's status information and RCSV also provides the specific certificate's status information. Therefore, the client can acquire the necessary information selectively.

4.5.6 Independence between Certification Authority and RCSV Server
If the clients only connect to the RCSV Server to validate the certificate status, s/he can get the CA’s CSI. The CA also need only one additional module to provide the CSI to the RCSV Server. Therefore the independent operation of the CA and the RCSV Server is possible.

As stated above, the proposed model can provide those properties to the CA, RCSV Server and the RCSV client. And it can be applied not only to certificate validation but to the additional service using extensions field.

Table 1. is the summary of the result examined so far.

<table>
<thead>
<tr>
<th>Schemes</th>
<th>T</th>
<th>R</th>
<th>L</th>
<th>D</th>
<th>S</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delta-CRL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Over-issued CRL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indirect CRL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OCSP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RCSV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Comparison of the each methods

5 Conclusions
PKI that needs a real-time CSI demands present point about status of certificate and real-time offer about status information of certificate. In this paper, we analyze the request items needed in this structure and propose a Real-time Certificate Status Validation Model With CSIProvider. For this, we provide a new protocol that the CA generates information of new certificate status and provides to the RCSV server through the CITT. RCSV server provides the CSI to the RCSV Client based on this information.

Real-time Certificate Status Validation Model With CSIProvider proposed in this paper reduces communication overload of both the CA and the user. And it is a suitable for the user who needs the CSI at the point of specific time. This system can give an additional support to both the user and the CA.

References: