情 報 保 護 學 會 誌
第 12 券 第 2 號, 2002. 4

온라인 인증서 상태 검증 프로토콜(OCSP)의 최근 연구 동향에 관한 분석

곽 진*, 이 승 우*, 조 석 향*, 원 동 호**

요 약

최근 전자상거래의 활성화 및 안전한 네트워크의 구현에 공개키 기반구조의 응용이 확대되면서 공개키의 무결성과 신뢰성을 제공하기 위해 공개키 인증서 상태 검증에 관한 연구가 활발히 진행되고 있다. 본 고에서는 PKI 응용 프로토콜 중에서 인증서의 유효성을 검증하기 위한 온라인 인증서 상태 검증 프로토콜(Online Certificate Status Protocol)의 최근 연구 동향에 대하여 분석하였으며, 현재 상용화되어 있는 제품들에 대하여 조사하였다. 또한, 특정 인증서에 대한 온라인 취소 상태 확인 서비스(ORS:Online Revocation Status), 인증 경로의 발견을 서버로 위임하는 대리 인증 경로 발견 서비스(DPD:Delegated Path Discovery), 그리고 중앙 집중 서버에게 인증 경로 검증의 기능을 위임하는 대리 인증 경로 검증 서비스(DPV:Delegated Path Validation) 등의 온라인 인증서 상태 검증 프로토콜에서 제공하는 서비스들에 대해서도 살펴보았다.

현재 온라인 인증서 상태 검증 프로토콜(OCSP)에 관한 문서는 IETF에서 표준화한 RFC2560과 2000년 11월과 2001년 3월에 제안된 드래프트가 있으며, 본 고에서는 RFC2560과 제안된 드래프트를 비교 분석하였으며 국내·외 제품의 동향과 온라인 인증서 상태 검증 프로토콜의 활용 범위에 대해서 간략하게 살펴보았다.

Ⅰ. 서 론

최근 급속하게 발전하고 있는 인터넷을 이용한 전자상거래가 활성화되면서 이를 이용한 금융, 증권 등의 분야에 응용되어 새로운 서비스들이 제공되기 시작하였다. 이러한 새로운 서비스들에서 제공되는 데이터의 기밀성과 통신 상대방의 인증을 위해 공개키 기반구조의 응용이 확대되었다.

공개키 기반구조를 이용한 서비스들은 서로 통신하는 상대방을 인증하거나 또는 거래 사실의 부인을 방지하기 위해 인증서를 사용하게 되었으며, 이 인증서는 사용하기 전에 반드시 검증 과정을 거쳐야 한다. 인증서의 검증 과정에서 인증서의 폐지상태 확인은 사용하고자 하는 인증서와 인증 경로상의 인증서들이 사용하고자 하는 시점에서 그 효력이 정지되었거나 폐지되었는지를 검사하는 것이다[2][3].

인증서 상태 검증을 위한 방법으로는 인증서 폐지목록(CRL:Certificate Revocation List) 방식, 인증서 폐지시스템(CRS:Certificate Revocation System), 인증서 폐지트리(CRT: Certificate Revocation Tree), 그리고 SCVP(Simple Certificate Validation Protocol) 등이 있는데 이 중 인증서 폐지목록(CRL) 방식을 주로 사용해 왔다. 하지만 이 방식은 인증서를 검증하고자 할 때마다 인증서 폐지목록 전체를 다운받아야 하고 인증서 폐지목록의 크기가 커질수록 다운받아야 하는 목록의 크기가 커짐에 따라 다운받는 시간과 통신량의 증가로 이어진다는 단점을 가지고 있다. 또한 기존의 인증서 상태 검증 방식들이 주로 주기적으로 발행되는 CRL에 기반을 두고 있기 때문에 인증서 현재 상태에 대한 time gap 문제가 발생할 수 있다[4][5].

이러한 기존의 인증서 상태 검증 방법들의 문제점으로 인해 최근 새로운 형태의 인증서 상태 검증 메커니즘이 제안되었으며 온라인 인증서 상태 검증 프로토콜(OCSP)이 대표적이라 할 수 있다.

현재 발표되고 있는 PKI 제품을 살펴보면 거의

* 성균관대학교 전기전자 및 컴퓨터공학부 정보통신보호연구실({jkwak,swlee,shcho}@dosan.skku.ac.kr)
** 성균관대학교 전기전자 및 컴퓨터공학부 (dhwon@simsan.skku.ac.kr)

대부분의 제품에서 OCSP의 기능을 제공하고 있으며 앞으로 더 많은 분야에서 활용될 것으로 보인다[6][7][8].

본 고에서는 1999년 6월에 IETF에서 표준화한 RFC2560과 2000년 11월과 2001년 3월에 새롭게 제안된 드래프트에 대해 분석하였으며, 특히 새로 제안된 드래프트를 중점으로 하여 온라인 인증서 상태 검증 프로토콜이 제공하는 서비스 부분에 대하여 분석하여 정리하였다.

본 고의 구성은 다음과 같다. Ⅱ장에서는 온라인 인증서 상태 검증 프로토콜(OCSP)의 구성에 대하여 알아보았으며, Ⅲ장에서는 온라인 인증서 상태 검증 프로토콜의 요구 메시지와 응답 메시지의 형식에 대하여 정리하였다. Ⅳ장에서는 온라인 인증서 상태 검증 프로토콜이 제공하는 3가지의 서비스에 대하여 정리하였으며, Ⅴ장에서는 최근 동향과 활용 범위에 대해 언급하고, 그리고 Ⅵ장에는 결론을 맺는다.

Ⅱ. 온라인 인증서 상태 검증 프로토콜 개요

온라인 인증서 상태 검증 프로토콜(OCSP)은 1999년 6월에 IETF에서 RFC2560으로 표준화되어 발표된 이래 현재까지 Internet Draft OCSP v2까지 발표되었다. 현재까지 IETF에서 발표된 OCSP 관련 문서를 표 1에 정리하였다.

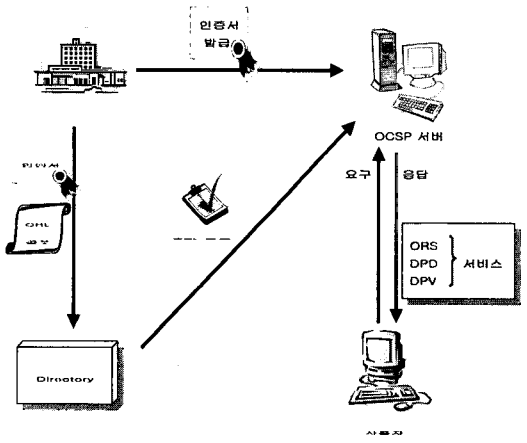
〔표 1〕 IETF PKIX OCSP 표준화 진행사항

발표/ 제출일시	문서 / 파일명
1999. 6	〔RFC2560 : Standard Track〕 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP
2000. 8	draft-ietf-pkix-ocsp-valid-00.txt
2000. 9	draft-ietf-pkix-ocsp-path-00.txt
2000. 11	draft-ietf-pkix-ocspv2-01.txt
2001. 3	draft-ietf-pkix-ocspv2-02.txt
2001. 7	draft-ietf-pkix-dpv-dpd-00.txt

인증서 검증 과정에서 인증 경로에 따라 클라이언트가 직접 인증서 폐지목록(CRL)을 획득하여 인증서의 유효성을 검증하는 프로토콜은 인증서의 유효성 검증을 위해 주기적으로 발행되는 CRL 전체를 다운받아야 하므로 시스템에 높은 부하를 주게 되고 이에 따른 통신비용의 발생, time gap 문제, 그리고 클라이언트가 자신이 사용하고 있는 인증서의 유효성 검증을 간결하게 처리하지 못하는 문제를 가지고 있다. 이러한 문제를 해결하기 위해 인증서 상태 정보를 검증할 수 있는 프로토콜로서 온라인 인증서 상태 검증 프로토콜(OCSP)이 제안되었다. OCSP는 온라인 상에서 OCSP 서버와 OCSP 클라이언트간에 수행되는 프로토콜로서 인증서의 효력정지 및 폐지상태를 CRL을 사용하지 않고 실시간으로 확인할 수 있게 해주는 프로토콜이다.

OCSP는 클라이언트가 온라인 취소 상태 확인 서비스(ORS), 대리 인증 경로 발견 서비스(DPD), 그리고 대리 인증 경로 검증 서비스(DPV) 등의 3가지의 상태 및 유효성 검증 서비스를 요구하고 서버가 이 요구 메시지에 대해 응답을 하는 프로토콜로서, 현재 IETF에서 제안하고 있는 Internet Draft OCSP v2는 구체적인 동작을 정의하고 있지 않으며 서버와 클라이언트간에 교환되는 메시지의 구성과 형태만을 정의하고 있다[9][10][11].

그림 1은 OCSP의 구조를 나타낸 것이다.



〔그림 1〕 OCSP의 구조

인증서는 클라이언트들의 공개키 정보와 이름을 바탕으로 하여 인증기관의 비밀키로 서명을 하게 되고, 이러한 과정을 통해 공개키에 대한 무결성을 제공해준다. 인증서를 사용하거나 서명문을 검증하고자 하는 클라이언트는 공개키에 대한 인증서의 유효성을 확인한 후 서명문에 대하여 검증을 하거나 인증서를 사용하여야 한다.

OCSP는 위에서 말한 3가지의 서비스를 사용하여 온라인 상에서 클라이언트가 서버에게 인증서의 취소 상태를 문의하거나 자신이 사용하고자 하는 인증서에 대한 인증 경로를 획득하거나 획득한 인증 경로에 대한 유효성을 검증할 수 있게 하는 프로토콜이다. 이 방식은 인증 경로 유효성 검증에 있어서 별도의 검증 서버인 OCSP 서버를 사용하여 인증 경로 검증을 수행한다. 서버는 인증기관이 자체적으로 운영하거나 별도의 신뢰 기관에 위임하여 운영할 수 있다. 별도의 신뢰 기관에 위임을 하기 위해서는 별도의 신뢰 기관에 인증서를 발행하여야 한다.

Ⅲ. 온라인 인증서 상태 검증 프로토콜의 데이터 구조와 요구사항

OCSP의 데이터 구조는 클라이언트가 서버로 보내는 요구 메시지(Request)와 서버에서 클라이언트에게 보내는 응답 메시지(Response)로 구성되며, 각각에 대하여 살펴보면 다음과 같다.

1. 요구 메시지 (OCSPRequest)

요구 메시지(OCSPRequest)는 클라이언트가 서버에게 특정 인증서의 상태 정보를 요구하는 메시지이다. 요구자가 서버에게 이 메시지를 보냈을 경우에는 서버의 응답 메시지(OCSPResponse)를 수신할 때까지 인증서의 유효성에 대한 판단을 보류하여야 한다.

요구 메시지의 구성은 크게 버전과 요구자의 이름 등을 포함하는 tbsRequest 필드와 서명 알고리즘 종류, 서명문, 그리고 서명에 사용된 서명용 키를 검증하기 위한 공개키의 인증 경로 등을 포함하는 optionalSignature 필드로 구성되어 있다.

그림 2는 요구 메시지의 구성을 그림으로 나타낸 것이며 각 필드들의 내용을 살펴보면 다음과 같다.

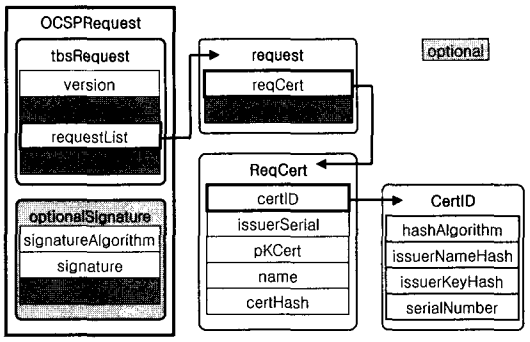
tbsRequest 필드는 크게 다음과 같은 필드로 구성되어 있으며, 각 필드들의 세부 내용은 다음과 같다.

- **version**

OCSP 프로토콜의 버전을 나타내며 디폴트(default) 값으로써 v1으로 표시된다.

- **requestorName**

옵션으로 처리되는 부분이며 request 요구자의 이름(General Name)을 나타낸다.



〔그림 2〕 요구 메시지(OCSPRequest)의 구성

- **requestList**

상태 검증을 요구하는 특정 인증서의 정보를 나타내는 필드로 ReqCert와 확장 영역을 나타내는 singleRequestExtensions으로 구성되어 있다.

- **ReqCert**

발급자의 고유번호를 나타내는 issuerSerial, 인증서를 나타내주는 pKCert, 이름을 나타내주는 name, CertHash, 그리고 certID 등의 선택사항으로 구성되어 있다.

- certID : 이 필드가 사용되면 버전은 v1으로 표시되며 다른 필드가 선택사항으로 사용되면 v2가 된다. certID는 다음의 4가지 필드로 구성되어 있다.
  - hashAlgorithm : 해쉬값을 생성하는데 사용하는 알고리즘의 식별자를 나타냄.
  - issuerNameHash : 발급자의 고유 이름(DN)에 대한 해쉬값을 나타냄.
  - issuerKeyHash : BIT STRING 값으로 표시되며 발급자의 인증서 내에 있는 공개키의 해쉬값을 나타냄.
  - serialNumber : 인증서의 일련번호를 나타냄.

- **singleRequestExtensions**

선택사항으로 처리되는 부분이며 요구 메시지의 확장 영역을 나타내는 필드이다.

- **requestExtensions**

OCSP 서버와 클라이언트간에 미리 합의된 확장 영역을 나타내주는 필드이며 옵션으로 처리되는 사

항이다. 이 필드가 하나 또는 그 이상의 값을 포함하고 있는 경우에 사용되며, 그렇지 않으면 OCSP Request 필드에서 생략되고, 이 경우에는 다음 장에서 설명하게 될 온라인 인증서 상태 검증 프로토콜이 제공하는 3가지의 서비스 중에서 ORS 서비스로 고려하게 되며, 나머지의 경우는 이 필드가 모두 요구된다.

optionalSignature 필드는 서명에 사용된 알고리즘의 식별자를 나타내는 signatureAlgorithm 필드, 서명을 포함하고 있는 signature 필드, 그리고 서명 검증에 사용될 공개키를 포함하고 있는 certs 필드로 구성되어 있다. 이 필드에는 서명에 관계된 정보가 포함되어 있으므로 사용될 경우에는 응답자에게 요구자의 서명 검증을 제공한다.

2. 응답 메시지 (OCSPResponse)

응답 메시지(OCSPResponse)는 클라이언트로부터 요구 메시지를 수신한 OCSP 서버가 요구된 인증서의 상태 검증 결과를 포함한 메시지를 클라이언트에게 전송하는 메시지이다.

응답 메시지도 요구 메시지와 마찬가지로 서명되어 전송되어야 하며 서명문을 생성하기 위해 인증서를 발급한 인증기관의 서명용 키를 이용한다. 클라이언트가 서버로부터 보내온 응답 메시지의 유효성을 검증하기 위해서는 공개키를 사용하기 전에 공개키 인증서의 유효성을 검증해야 하며 서명문을 검증하기 위해 사용되는 서버의 공개키는 인증서의 형태로 클라이언트에게 전송하게 된다.

응답 메시지는 CRL이나 CRS, 그리고 CRT 방식 등과 같은 기존의 인증서 경로 검증 프로토콜에서의 문제점을 보완하기 위해 클라이언트의 요구가 있을 경우 이를 처리할 수 있는 기본적인 능력이 요구되며 인증서의 상태를 검색하고 서명하는 시간을 최소화할 수 있는 방법으로 인증서의 현재 상태에 대한 응답을 제공하여 인증서의 상태를 온라인 상에서 실시간으로 확인할 수 있도록 제공해 주어야 한다.

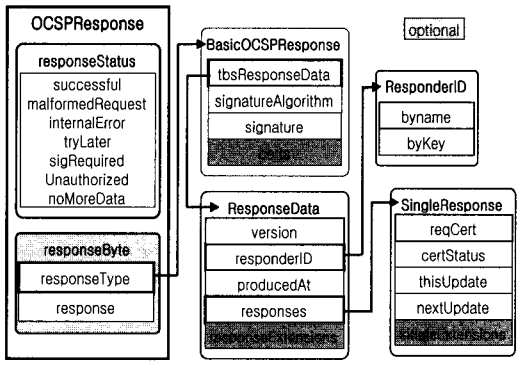
응답 메시지의 구성은 크게 응답의 상태를 나타내는 responseStatus 필드와 구체적인 응답의 내용을 나타내주는 responseByte 필드로 구성되어 있다. 응답 메시지의 최소 구성은 responseStatus 필드만으로 구성이 가능하다.

그림 3은 응답 메시지의 구성을 나타낸 것이며 각 필드들의 내용을 살펴보면 다음과 같다.

responseStatus 필드는 다음의 7가지 내용으로 인증서의 상태를 나타내준다.

- **successful**

〔0〕으로 표시되며 이 값으로 표시가 되면 response Byte 필드가 구성되며, 그렇지 않을 경우에는 response Byte 필드가 구성되지 않은 상태로 응답 메시지가 구성된다.



〔그림 3〕 응답 메시지(OCSPResponse)의 구성

- **malformedRequest**

〔1〕로 표시되며 요구자의 요구 메시지가 합당하지 않은 잘못된 형식임을 나타낸다.

- **internalError**

〔2〕로 표시되며 요구 메시지가 서버 내부의 상태에 일치하지 않는 내부 오류 상태임을 나타낸다.

- **tryLater**

〔3〕으로 표시되며 서버가 작동은 하고 있지만 인증서 상태를 알려줄 수 없는 경우에 사용되는 것으로, 서비스는 존재하지만 일시적으로 응답할 수 없는 경우에 사용됨을 나타낸다.

- **sigRequired**

〔5〕로 표시되며 응답 메시지를 구성하기 위해 요구자 서명을 요구하고 있음을 나타낸다.

- **unauthorized**

〔6〕으로 표시되며 요구자가 권한이 부여되지 않은 경우를 나타낸다.

- **noMoreData**

〔7〕로 표시되며 새롭게 드래프트에 추가된 부분

으로 요구 메시지와 관계된 결과에 대해 이미 응답을 해준 경우에 사용된다.

위의 내용을 간략하게 정리하면 다음의 표 2와 같다.

〔표 2〕 인증서 상태 표시 메시지

상 태 표 시	설 명
successful〔0〕	상태 검증 성공
malformedRequest〔1〕	잘못된 형식의 요구 메시지
internalError〔2〕	내부 오류 발생
tryLater〔3〕	상태를 알려줄 수 없음
sigRequired〔5〕	요구자의 서명을 요구
unauthorized〔6〕	요구자 권한 부여되지 않음
noMoreData〔7〕	이미 응답을 해준 경우

responseByte 필드는 응답 메시지의 유형을 나타내는 responseType과 response로 구성되어 있으며 responseType은 다음과 같이 BasicOCSPResponse로 정의되어 있으며 각각의 내용을 살펴보면 다음과 같다.

- **BasicOCSPResponse**

응답 메시지의 구성에 이 필드를 사용하기 위해 responseType을 id-pkix-ocsp-basic으로 표시하여야 한다. 이 필드는 응답 메시지의 자세한 정보를 포함한 tbsResponseData와 서명에 사용된 알고리즘을 나타내는 signatureAlgorithm 필드, 서명을 포함하고 있는 signature 필드, 그리고 서명 검증에 사용할 공개키를 포함하고 있는 certs 필드로 구성되어 있다.

- **tbsResponseData**

응답 메시지의 버전과 응답 메시지 생성 시간 등 응답 메시지와 응답자의 정보를 담고 있는 tbs ResponseData 필드의 각 내용을 살펴보면 다음과 같다.

- version : 응답 메시지의 버전을 나타내며 v1으로 표시됨.
- responderID : 선택사항으로 응답자의 식별정보를 byname과 byKey로 나타냄. name을 사용하는 경우는 〔1〕, 응답자의 공개키 해쉬값으로 나타내는 경우는 〔2〕로 표시함.
- producedAt : 응답 메시지의 생성 시점으로 응답 메시지에 대해 응답자가 서명한 시간을 나타내는 것으로 GeneralizedTime으로 나타냄.
- responses : singleResponse로 정의가 되는 부분이며, reqCert와 특정 인증서의 상태를 나타내는 certStatus, 인증서 상태의 유효한 시간을 나타내는 thisUpdate와 nextUpdate, 그리고 확장 영역을 나타내는 singleExtensions 필드로 구성되어 있으며, nextUpdate 필드가 사용되지 않으면 응답자는 새로운 취소 정보가 모든 시간에 대해 유효한 것으로 나타냄.
- responseExtensions : 확장 영역을 나타내며 선택사항임.

- **certStatus**

특정 인증서의 상태를 나타내며 "good", "revoked", 그리고 "unknown"으로 나타낸다.

- "good" 상태 : 〔0〕으로 표시하며 긍정적인 응답을 표시하는 것으로 인증서의 상태가 취소되지 않았음을 나타냄. 인증서의 발행 또는 인증서의 유효 기간을 나타내는 것은 아님.
- "revoked" 상태 : 〔1〕로 표시하며 인증서의 상태가 영구적 또는 일시적으로 취소되었음을 나타냄.
- "unknown" 상태 : 〔2〕로 표시하며 인증서의 취소 여부에 대하여 응답자가 알지 못할 경우를 나타냄.

- **응답메시지의 시간정보**

OCSP 응답 메시지에서는 세 가지의 시간 정보를 제공하고 있다. 이 시간들은 응답 메시지에 포함되어 있는 정보에 대한 유효기간을 판단할 수 있는 근거로 사용될 수 있으며, thisUpdate, nextUpdate, 그리고 producedAt 등이 있다.

- thisUpdate : 응답 메시지의 상태정보가 유효하다고 가리키는 시각
- nextUpdate : 새로운 상태정보가 가능할 것이라는 시각
- producedAt : OCSP 서버가 해당 응답에 서명한 시각

이러한 시간 정보 중에서 nextUpdate 시간 정보가 설정되지 않으면 서버는 언제라도 새로운 폐기 정보를 가리킬 수 있다는 것을 의미한다.

3. 온라인 인증서 상태 검증 프로토콜의 기본적 요구사항

OCSP는 온라인으로 인증서의 상태를 확인할 수 있도록 서비스하기 위해 두 가지의 기본적인 요구사항을 포함하고 있다.

OCSP 서비스를 제공하고 있는 인증기관은 서비스를 이용하는 클라이언트들이 정보를 얻을 수 있는 곳을 전달하기 위해 인증서에 OCSP 서버의 위치를 알려주는 정보를 포함하여야 한다. 이를 위해서 인증서에는 클라이언트들이 OCSP의 위치를 명확하게 확인할 수 있도록 하기 위해 AuthorityInfoAccess 확장 필드를 지원해야 하며, HTTP 방식 등 OCSP 서버에 접근하는 방식과 URL등과 같은 부가적인 정보를 포함한 AccessLocation 값을 지원하여야 한다.

또한, 클라이언트들은 응답 메시지를 수락하기 전에 전송 받은 응답 메시지에 포함되어 있는 인증서 식별자가 자신이 요구한 메시지에 포함된 것과 동일한지의 여부와 메시지에 대한 서명, 자신이 서비스를 요구한 OCSP 서버가 정확한지, 그리고 응답 메시지의 thisUpdate와 nextUpdate 정보가 올바르게 작성이 되었는지의 여부를 확인하여야 한다.

Ⅳ. 온라인 인증서 상태 검증 프로토콜 서비스

RFC2560에서 제안한 OCSP는 온라인 인증서 상태에 대한 인터넷 표준을 제정하고 있으며 현재 발표되고 있는 OCSP v2는 클라이언트가 온라인 상에서 특정 인증서의 상태를 OCSP 서버에게 문의하거나 그에 대한 인증 경로를 획득 가능하게 하고 획득한 인증 경로의 유효성에 대해 검증할 수 있는 프로토콜로 제안되었다.

OCSP v2가 포함하고 있는 서비스로는, 온라인 취소 상태 확인 서비스(ORS), 대리 인증 경로 검증 서비스(DPV), 그리고 대리 인증 경로 발견 서비스(DPD) 등이 있으며 각각에 대하여 살펴보도록 하겠다.

1. 온라인 취소 상태 확인 서비스 (Online Revocation Status)

온라인 취소 상태 확인 서비스(ORS)는 클라이언트가 서버에게 특정 인증서의 정보를 제공하고 서버는 클라이언트에게 특정 인증서의 취소 상태를 검사하여 알려주는 것으로, RFC2560에서 제안된 OCSP v1과 거의 비슷하다고 할 수 있다. 또한 이 서비스는 CRL 형식을 따르지 않는다.

ORS 서비스를 사용하기 위해서는 클라이언트와 서버 사이의 메시지 형식이 id-pkix-ocsp-basic response type의 형태이어야 하며 양측 모두에게 이러한 형태의 필드 처리 능력이 요구된다.

1.1 ORS 서비스 요구 (Request)

ORS 서비스를 요구하기 위한 요구 메시지의 형식은 OCSP 요구 메시지를 따르고 있으며 서명하여 전송해야 한다.

클라이언트의 요구 메시지에는 ORS 서비스를 사용하기 위해 OCSPRequest의 tbsRequest 필드에 옵션으로 처리되는 requestExtensions 필드 부분에 id-pkix-ocsp-ors-req의 OID 값이 포함되어 있어야 한다.

이를 수신하는 서버도 마찬가지로 요구 메시지에 포함된 id-pkix-ocsp-ors-req OID 값을 인식하고 처리할 수 있어야 한다.

1.2 ORS 서비스 응답 (Response)

ORS 서비스 요구에 대한 응답 형식은 위에서도 언급한 바와 같이 id-pkix-ocsp-basic response type의 형태이어야 하며, 이에 대한 응답의 내용은 BasicOCSPResponse 필드에 구성된다.

ORS 서비스의 응답 메시지는 "good", "revoked", 그리고 "unknown" 등의 3가지 상태로 구성된다.

- "good" 상태 : [0]으로 표시하며 긍정적인 응답을 표시하는 것으로 인증서의 상태가 취소되지 않았음을 나타냄.
- "revoked" 상태 : [1]로 표시하며 인증서의 상태가 영구적 또는 일시적으로 취소되었음을 나타냄.
- "unknown" 상태 : [2]로 표시하며 인증서의 취소 여부에 대하여 응답자가 알지 못할 경우를 나타냄.

[표 3] ORS 서비스 인증서 상태 표시 메시지

상 태 표 시	설 명
good [0]	인증서 유효
revoked [1]	인증서 취소
unknown [2]	인증서의 상태 인식 불가

2. 대리 인증 경로 검증 서비스 (Delegated Path Validation)

대리 인증 경로 검증 서비스(DPV)는 클라이언트가 특정 인증서의 경로 검증 기능을 서버에게 위임하는 프로토콜로서 클라이언트 측의 비용을 감소시켜주는 프로토콜이다.

클라이언트가 특정 인증서의 상태를 검증하기 위해 인증서의 정보를 서버에게 보내고 서버는 수신한 인증서의 정보를 바탕으로 인증 경로의 유효성을 검증하고 그 결과와 정보를 클라이언트에게 응답해주는 과정으로 이루어져 있다.

DPV 서비스는 구성원들에게 인증기관의 인증서를 발급하고 구성원들은 발급 받은 인증서를 최종 사용자에게 발급하는데 사용이 가능하고 산업 공동체의 구성과 같은 구조에서 인증서의 기술적인 부분을 감소시키며 인증서 경로 과정의 통합을 쉽게 할 수 있는 장점을 가지고 있다.

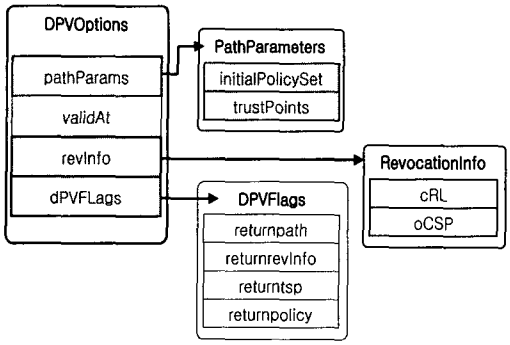
2.1 DPV 서비스 요구 (Request)

클라이언트가 DPV 서비스를 요구하기 위해서는 tbsRequest 필드의 requestExtensions 확장 필드에 id-pkix-ocsp-valid-req의 OID 값과 DPV Options의 값을 가지고 있어야 한다.

그림 4는 DPVOptions의 구성을 나타낸 것이다.

2.2 DPV 서비스 응답 (Response)

클라이언트의 DPV 서비스 요구에 대한 서버의 응답은 ResponseByte의 ResponseType 필드에 id-pkix-ocsp-valid-rsp 값을 포함하고 있어야 하며 응답의 내용은 위에서 언급한 ORS 서비스와 마찬가지로 BasicOCSPResponse 필드에 구성된다.



〔그림 4〕 DPVOptions 필드의 구성

인증서 상태에 대한 응답은 BasicOCSP Response 필드의 DPVCertStatus에 "valid", "invalid", 그리고 "unknown"으로 구성된다.

- "valid" 상태 : 〔0〕으로 표시하고 인증 경로가 유효함을 나타냄.
- "invalid" 상태 : 〔1〕로 표시하며 인증 경로가 유효하지 않음을 나타내고, 경로 검증에 있어서 몇몇 조건이 불충분함을 나타냄.
- "unknown" 상태 : 〔2〕로 표시하며 인증 경로 과정에서 서버가 개체들의 인증서에 대해 인식하지 못함을 나타냄. 서비스 요구 메시지의 trustPoints 옵션이 NULL 값이 아닌 다른 값을 포함하고 있다면 서버는 그 값에 해당하는 trustPoints를 검증하게 되는데 그 결과 인증 경로를 생성하지 못하면 인증 경로 상태를 "unknown" 상태로 표시하게 됨

〔표 4〕 DPV 서비스 인증 경로 상태 표시 메시지

상 태 표 시	설 명
valid 〔0〕	인증 경로 유효
invalid 〔1〕	인증 경로 유효하지 않음
unknown 〔2〕	알 수 없음

3. 대리 인증 경로 발견 서비스 (Delegated Path Discovery)

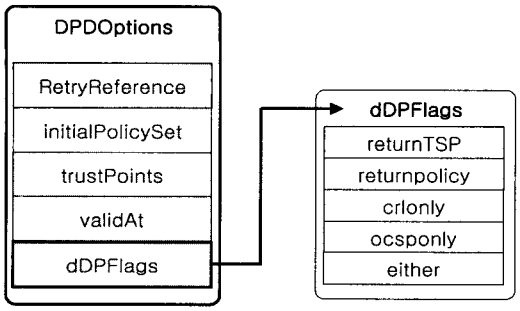
대리 인증 경로 발견 서비스(DPD)는 인증 경로 발견의 기능을 서버로 위임하여 인증 경로가 다양하게 존재하는 경우 신뢰할 수 있는 경로를 서버가 선택할 수 있도록 하는 프로토콜이다.

OCSP 요구 메시지에 대한 DPD 서비스도 앞서 기술한 ORS와 DPV 서비스와 마찬가지로 OCSP 요구 메시지의 requestExtensions 필드에 적용된다.

3.1 DPD 서비스 요구 (Request)

DPD 서비스를 요구하기 위해서는 ORS 서비스와 DPV 서비스를 요구할 때와 마찬가지로 tbs Request의 requestExtensions 필드에 DPD 서비스를 위한 id-pkix-ocsp-path-req의 OID 값과 RetryReference의 값을 포함하여야 한다.

그림 5는 DPDOptions의 구성을 나타낸 것이다.



〔그림 5〕 DPDOptions 필드의 구성

RetryReference는 이전의 응답을 기반으로 하는 서버에게 유효한 경로 획득을 가능하게 한다. 클라이언트가 RetryReference를 명시하면 응답자는 해당 정보와 함께 이전에 응답하였던 어떠한 경로에 대해서도 반환하지 않는다.

3.2 DPD 서비스 응답 (Response)

클라이언트의 DPD 서비스에 대한 서버의 응답 또한 ORS 서비스와 DPV 서비스 응답과 마찬가지로 ResponseByte의 ResponseType 필드 부분에 id- pkix-ocsp-path-rsp 값을 포함하고 있어야 한다.

이 서비스의 응답은 클라이언트가 보낸 요구 메시지의 tbsRequest의 requestList 필드 내에 포함된 각각의 인증서에 대해서 응답 메시지를 구성하며 최종 사용자 인증서와 최종 CA 인증서까지 순서대로 구성하여야 한다.

V. 최근 동향 및 활용 범위

1. OCSP 최근 동향

본 절에서는 국·내외에서 개발되고 있는 PKI 제품을 통해 OCSP가 실제 PKI 제품에서 어떻게 적용되고 있는지 살펴보도록 한다.

1.1 국내 제품 동향

현재 국내에서도 공개키 기반구조의 연구가 활발히 진행되면서 PKI 제품이 계속해서 발표되고 있다.

본 절에서는 소프트포럼(주)의 XecurePKI와 펜타시큐리티시스템(주)의 ISSAC-VA, 그리고 KSign의 KSignOCSP에 대하여 간략하게 살펴보도록 한다.

- **XecurePKI**

소프트포럼(주)의 XecurePKI는 국내 공개키 기반구조 분야에서 절반이상의 시장점유율을 차지하고 있는 업체로서 금융권과 정부부처, 민간기업 등을 확보하고 있으며 금융결제원이 공인 인증기관 서비스 파트너로 선정한 업체이다. XecurePKI는 데이터 암호, 사용자 인증, 전자서명을 통하여 인터넷을 기반으로 하는 전자상거래에 신뢰성을 제공하기 위한 보안솔루션으로 사용자에게 디지털 인증서를 발급하여 사용자의 신원을 증명하고 인증서에 기반한 전자서명을 구현함으로써 데이터 무결성과 거래사실 부인방지 기능을 제공한다.

본 제품에서는 인증서의 폐지여부를 OCSP 서버를 통해 온라인으로 조회하는 XecureOCSP 시스템을 사용하고 있다. 사용자의 인증 서비스를 제공할 때 사용자 인증서의 유효성 검증을 위해 OCSP를 운영할 수 있으며 그렇지 않을 경우에는 인증서 폐지목록(CRL)을 이용한 기존 방식을 지원한다.

XecureOCSP는 CA로부터 사용자 인증서 유효성 검증 기능을 위임받아 인증기관을 대신하여 사용자 인증서의 유효성에 대한 신뢰된 서비스를 제공하고 있다. 인증기관은 인증서 폐지목록을 발급할 경우 주기적인 작업을 통해 발급하고 있으며 인증서 폐지목록 자체의 유효기간을 선정하여 사용자들에게 공지하고 인증서 폐지목록의 발급 위치 및 OCSP의 위치를 인증서에 첨부하여 사용자들의 검증 서비스를 지원한다. 또한, 온라인 인증서 상태 등을 조회하고 게시하는 기능을 제공하는 XecureCDS(Certificate Distribution System)와 연동하여 실시간 인증서 상태 조회 서비스를 제공한다.

- **ISSAC-VA**

펜타시큐리티시스템(주)에서 개발한 PKI 제품은 인증서 발급 및 관리 시스템인 ISSAC-CA, CA의 기능 중 사용자 등록·관리와 관련된 기능을 하는 ISSAC-RA, 인증서 및 인증서 폐지목록을 저장하는 디렉토리 서버, 사용자의 비밀키를 복구해 주는 ISSAC-KMS, 인증서의 발급·갱신·폐지 등과 관련되는 사용자 프로그램인 ISSAC-client, 그리고 인증서의 유효성에 대한 정보를 사용자에게 서비스하는 ISSAC-VA의 시스템으로 구성되어 있다.

ISSAC-VA는 인증서 검증 서비스 중 인증서의 효력정지나 폐지 여부를 온라인으로 확인하는 OCSP 시스템으로 온라인 상에서 실시간으로 인증서 검증에

필요한 인증서의 폐지 상태 확인을 클라이언트와 서버간의 간단한 요구와 응답을 통해 수행한다.

본 제품의 특징은 인증기관에서 서명한 권한을 위임받아 시스템을 분리하고 인증기관에 독립적으로 서비스를 제공하여 타사의 인증기관과 연동이 가능한 독립적인 시스템(Independent System Operation)을 운영하고 있다는 것이다.

- **KSignOCSP**

KSign은 PKI 솔루션 전문 업체로서 공인인증기관인 한국전산원과 한국정보인증(주)에 PKI 인증 시스템을 구축해 성능과 안전성을 인정받았다.

KSign의 PKI 인증 솔루션인 KSignPKI는 인증서 생성관리 시스템인 KSignPKI CA와 등록관리 시스템인 KSignPKI LRA, 클라이언트 시스템인 KSignPKI Client, KsignRA, KsignTSA, 그리고 KSignOCSP등을 제공하고 있다.

KSignOCSP 서버는 인증서 폐지 목록을 통한 인증서 검증 메커니즘과 함께 서비스의 다양화를 제공할 수 있는 기존의 인증서비스와 연동이 가능하며, OCSP 서비스 사용자의 증가에 따라 다수의 OCSP 서버를 운영하여 안정적인 서비스의 제공이 가능하다는 특징을 가지고 있다.

1.2 국외 제품 동향

국외 PKI 제품에서 제공하는 OCSP 서비스의 동향을 알아보기 위해 본 절에서는 ValiCert사의 ValiCert VA, VeriSign의 OnSite, Entrust사의 Entrust 6.0, 그리고 Baltimore사의 UniCERT 3.5에 대하여 간략하게 살펴보도록 한다.

- **ValiCert VA**

인증서 확인 및 디지털 영수증 솔루션 업체로 유명한 ValiCert사의 본 제품은 국·내외에서 가장 많은 사용자를 보유하고 있는 PKI 솔루션 업체인 Entrust사와 Baltimore사가 OCSP 서비스를 제공하기 위해 채택하고 있는 제품이다.

주요 인증서 검증 프로토콜을 지원하기 위해 OCSP 뿐만 아니라 CRL 등도 지원하고 있으며 검증 요구를 수행하기 위한 OCSP 요구는 권한이 부여된 클라이언트만이 수행할 수 있도록 전자서명이 가능하다.

- **OnSite**

IETF를 통해 OCSP를 처음 제안한 VeriSign의 제품인 OnSite는 인증서 검증 모듈인 CVM (Certificate Validation Module)을 포함하고 있다.

CVM은 인증서 체인 및 효력정지, 폐지 상태 검사를 포함하는 완전한 인증서 검증을 수행한다.

OnSite에서 제공하는 OCSP 서비스는 가상 사설 네트워크(Virtual Private Network), 온라인 경매, 금융 기관 등에서 VeriSign이 발행한 모든 인증서에 대해 그 유효성을 실시간으로 검증할 수 있다.

- **Entrust 6.0**

Entrust사의 PKI 제품은 ValiCert의 검증 서비스를 사용하여 OCSP를 지원하고 있다. 이를 통해 기존의 인증서 폐지목록(CRL) 또는 인증서 폐지목록 분배지점(distribution point)을 사용하여 제공한 인증서 검증 서비스에 부가적으로 실시간 인증서 효력정지 및 폐지목록을 검증할 수 있는 OCSP 서비스를 제공하고 있다.

- **UniCERT 3.5**

UniCERT는 강력한 인증기관과 유용한 정책 기반 관리 기능을 지원하는 PKI 제품으로 클라이언트 지원이 미약하여 하드웨어 토큰을 사용하지 않으면 다른 시스템에서 사용하는 것이 어려운 단점을 가지고 있지만 강력한 정책 편집기를 사용해 인증 생성에 필요한 정보관리에 대한 강력한 제어를 지원하고 있다. ValiCert사의 ValiCert VA 제품을 채택하여 OCSP 서비스를 제공하고 있다.

2. OCSP 활용 범위

인터넷을 이용한 금융, 증권, 전자상거래 등의 새로운 서비스들이 제공되기 시작하면서 공개키 기반구조가 확산되기 시작하였다. 공개키 기반구조를 이용한 서비스들에서 인증서가 큰 역할을 하게 되었으며, 인증서는 사용 전 반드시 검증 과정을 거쳐야 한다.

OCSP는 인증서 상태 정보를 실시간으로 제공해 주는 서비스로 최종 사용자의 인증서 상태 검증의 부담을 제거해 주고 간단한 요구 메시지와 응답 메시지를 통해 실시간으로 클라이언트가 필요로 하는 인증서의 상태 정보를 제공하므로 신속한 처리가 요구되는 금융 서비스, 공공기관 서비스, 전자상거래, 그리고 무선 인터넷 서비스 등에서 유용하게 사용될

수 있다.

2.1 금융 서비스

인터넷의 발달과 함께 시간과 장소에 부담을 가지지 않고 거래를 할 수 있는 편이성과 금융기관과 고객사이의 비용을 절감할 수 있는 경제성으로 전자금융은 급속도로 발전하고 있다.

현재 국내 인터넷 뱅킹 사용자는 2001년 1월 400만을 넘어 점차 증가하고 있는 추세이다. 이러한 전자금융 서비스가 정착하기 위해서는 서비스의 신뢰성과 안전성, 보안성이 매우 중요하며 이 때문에 SSL과 TLS 등의 보안 프로토콜을 이용하여 서비스를 제공하고 있다. 이러한 서비스 과정 또한 인증서를 사용하기 때문에 인증서의 검증과정이 수행되어야 하며, OCSP 서비스를 사용하여 실시간으로 인증서의 상태를 검증하게 된다면 사용자들은 인증서 상태 정보를 쉽게 얻을 수 있을 것이며, 수많은 사용자들을 대상으로 서비스를 제공하는 경우 통신량을 줄일 수 있을 것이다.

2.2 공공기관 서비스

인터넷의 활성화로 민원인 허가 서류 발급이나 각종 증명서 발급 등의 서비스도 인터넷을 통한 전산화가 활발히 진행되고 있다. 또한 여러 전자 입찰이나 조달 업무 역시 전산화가 이루어지고 있다.

이러한 서비스는 공공기관과 민간의 전자적인 업무처리에 있어 신뢰와 안전성이 보장되어야 하고 상호인정의 문제가 선결되어야 가능하므로 이를 위한 암호체계와 인증기반의 마련이 필요하다. 특히 민원 관련 업무의 경우는 다수의 국민을 대상으로 제공되는 서비스이므로 인증서의 상태 정보를 제공해 주는 OCSP 서비스의 활용이 유용할 것이다.

2.3 전자상거래 서비스

기업과 기업, 기업과 개인 등의 사이에서 이루어지는 전자상거래에서는 인증서에 기반한 인증, 인증상태의 실시간 검증들을 포함하는 최상의 보안성이 요구된다. 특히 전자상거래의 경우 개인의 신용정보와 금융기관과의 거래정보 등이 온라인 상에서 주를 이루기 때문에 서비스의 안전성과 신속성이 매우 중요한 역할을 한다. 때문에 OCSP 서비스를 활용하여 실시간으로 인증 상태의 검증이 제공되어야 할 것이다.

2.4 무선 인터넷 서비스

무선 인터넷은 장소에 관계없이 접속이 가능하다는 장점과 다양한 미디어 컨텐츠와 장비들의 발달로 인해 급속도로 발전할 것으로 예상되고 있다. 그렇기 때문에 유선 환경에서만 이루어지던 전자상거래도 무선 환경으로 점차 확산될 것으로 전망하고 있다.

무선 환경에서도 유선 환경에서와 마찬가지로 전자상거래를 위한 보안이 필수적으로 요구되며 이러한 보안 문제의 해결이 선결되지 않고서는 무선에서의 전자상거래는 불가능할 것이다. 특히 무선 환경에서는 인증서의 상태 검증 요청과 같은 작업이 유선 환경에서와는 달리 소형 단말기를 주로 사용하기 때문에 클라이언트 측의 비용 최소화가 요구된다.

현재 무선 인터넷은 ME 방식과 WAP 방식이 주를 이루고 있으며 ME 방식은 SSL 프로토콜을, WAP 방식은 WTLS를 사용하고 있으며 WAP용 인증서는 X.509 v1 인증서에 약간의 확장 필드가 추가된 형태를 가지고 있다. 이는 무선 인터넷의 처리 속도와 용량 등의 문제를 고려한 것이다. 그렇기 때문에 OCSP 서비스를 활용하면 속도와 용량의 비효율적인 면을 개선할 수 있을 것이다.

Ⅵ. 결 론

본 고에서는 온라인 상에 실시간으로 인증서의 상태 정보를 제공할 수 있는 OCSP의 형식과 구성, 그리고 동향과 활용 범위에 대하여 간략하게 알아보았다.

인터넷의 발달과 함께 전자상거래가 활성화되고 안전한 네트워크 환경의 구현에 공개키 기반구조의 응용이 확대됨에 따라 통신에 있어서의 신뢰성을 충족시키기 위해 인증서가 사용되었다. 이러한 인증서의 사용이 증가함에 따라 인증서의 효력정지 및 폐지상태에 관한 정보를 효율적으로 제공하기 위한 연구가 활발히 진행되고 있으며, 그 결과로 OCSP가 발표되었다.

앞에서도 살펴보았듯이 OCSP는 여러 분야에서 유용하게 활용될 수 있으며 금융기관 서비스, 공공기관 서비스, 전자상거래, 그리고 무선 인터넷의 발달과 함께 공개키 기반구조를 필요로 하는 네트워크 환경에 적용할 수 있다. 그러나 OCSP 방식은 CA의 디렉토리 접근에 의한 과부하 발생과 다른 인증서 상태 검증 방식과의 연동 문제 등을 가지고 있으며, OCSP 서비스 또한 CRL 방식을 완전히 배제

하지 못하기 때문에 응답과 요구에 있어서 응답 메시지의 현재성과 인증서의 상태 검색 및 응답 메시지에 대한 서명 작업으로 인해 실시간으로 응답을 제공할 수 있는가에 대한 문제를 가지고 있다. 그러므로 이를 해결하기 위한 연구가 필요하며 실제 시스템에 적용할 수 있도록 더 많은 연구가 진행될 것으로 기대된다.

참 고 문 헌

[1] W.Diffie and M.Hellman. "New Directions In Cryptography". IEEE Trans on Information Theory, vol.IT-22, pp.644-654. Nov.1976

[2] ISO/IEC 9594-8. "Information techno logy Open System Interconnection The Directory : Authentication Frame work", X.509, June.1997

[3] R.Housley, W.Ford, W.Polk, D. Solo. RFC2459 "Intranet X.509 Public Key Infrastructure Certificate and CRL Profile". Jan.1999

[4] M.Naor, K.Nissim. "Certificate Revocation and Certificate Update. In proceeding of the 7th USENIX Security Symposium. pp217-228. Jan, 1998

[5] P.McDaniel, S.Jamin. "Windowed Certificate Revocation". Technical Report. CSETR-413-99, EECS. University of Michigan. Ann Arbor. Nov.1999

[6] M.Myers, R.Ankney, A.Malpani, S. Galperin, C.Adams. RFC2560 "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP". IETF Standard. June.1999

[7] M.Myers, R.Ankney, C.Adams. "Online Certificate Status Protocol, version2". IETF Draft, draft-ietf-pkix-ocspv2-01. txt. Nov.2000

[8] M.Myers, R.Ankney, C.Adams. S.Farrell. "Online Certificate Status Protocol, version 2". IETF Draft, draft-ietf-pkix-ocspv2-02.txt. Mar, 2001

[9] M.Myers, S.Farrell, C.Adams. "Delegated Path Discovery with OCSP". IETF Draft, draft-ietf-pkix-ocsp-path-00.txt. Sep.1999

[10] M.Myers, C.Adams, S.Farrell. "Delegated Path Validation". IETF Draft, draft-ietf-pkix-ocsp-valid-00.txt. Aug, 2000

[11] D.Pinkas. "Delegated Path Validation and Delegated Path Discovery Protocols". IETF Draft, draft-ietf-pkix-dpv-dpd-00.txt. Jul.2001

〈著 者 紹 介〉

곽 진 (Jin Kwak)
학생회원
2000년 8월 : 성균관대학교 바이오메카트로닉스공학과 공학사
2001년 3월~현재 : 성균관대학교 전기전자 및 컴퓨터공학부 석사과정

이 승 우 (SuengWoo Lee)
학생회원
2001년 3월 : 강남대학교 전자계산학과 공학사
2001년 3월~현재 : 성균관대학교 전기전자 및 컴퓨터공학부 석사과정

조 석 향 (SeokHyang Cho)
학생회원
1986년 2월 : 이화여자대학교 수학과 이학사
1986년 9월~1998년 5월 : 중앙교육진흥연구소 선임 연구원
2001년 2월 : 서울산업대학교 전자계산학과 공학석사
2001년 3월~현재 : 성균관대학교 전기전자 및 컴퓨터공학부 박사과정

원 동 호 (DongHo Won)
종신회원
성균관대학교 전자공학과 (학사, 석사, 박사)
한국전자통신연구소 전임연구원
일본동경공대 객원 연구원

성균관대학교 교학처장, 전기전자 및 컴퓨터공학부
장, 정보통신대학원장,
국무총리실 정보화추진위원회 자문위원
한국정보보호학회 이사, 부회장, 수석부회장
현재 성균관대학교 전기전자 및 컴퓨터공학부 교수
한국정보보호학회 회장
정통부지정 정보보호인증기술연구센터 센터장