DPD/DPV 프로토콜 요구기준을 만족하는 개선된 OCSP (I-OCSP) 설계

박종욱° 서정훈 이 용 이재일
한국정보보호진흥원 전자서명인증관리센터
{khopri°, sjhoon, ylee, jilee}@kisa.or.kr

Design of the Improved OCSP (I-OCSP) satisfying the DPD/DPV protocol requirements

Jong-Wook Park° Junghoon Suh Yong Lee Jaeil Lee
Korea Certification Authority Central, Korea Information Security Agency

요 약

본 고에서는 현재 X.509 인증서를 검증하기 위하여 온라인으로 인증서 상태정보를 제공하는 OCSP가 클라이언트·프로토콜·서버 주체별로 IETF 공개키기반구조 워킹그룹에서 정의한 총 23개의 DPD/DPV 프로토콜 요구기준에 적절히 부합하는지 고찰하고 도출된 기술적 보완사항을 적용하여 다양한 응용환경에 적합하며 신뢰성 있는 서비스를 제공할 수 있는 개선된 OCSP를 제시하고자 한다.

1. 서 론

1970년대 공개키기반구조(PKI, Public Key Infrastructure) 개념이 나온 이래 현 시점의 주요 이슈는 글로벌한 환경에서 여러 인증경로를 갖는 인증서에 대한 효율적인 인증경로탐색과 획득된 인증경로를 구성하는 인증서들에 대한 인증경로검증이다. 특히 핸드폰이나 PDA와 같은 무선단말기 클라이언트는 한정된 자원과 연산처리부하로 경로탐색과 경로검증을 동시에 처리하는 것이 어렵다. 결국 이러한 상황은 인증서비스의 품질저하를 초래하게 되는 원인이 된다. 이에 대한 대안으로 클라이언트 대신 서버가 상기 기능을 대리수행 하는 DPD (Delegated Path Discovery, 위임경로탐색)와 DPV (Delegated Path Verification, 위임경로검증) 프로토콜 개념이 등장하였다. 즉, 인터넷 표준화단체인 IETF PKIX 워킹그룹은 DPD/DPV 서버가 프로토콜·중계관리·인증정책관리 측면에서 갖추어야 조건을 정의하여 클라이언트의 경량화와 인증서 검증 관련 서비스의 통일화를 도모하고 있다[1]. 한편 OCSP는 CRL없이 실시간으로 인증서 상태정보를 검증할 수 있는 효과적인 방법으로 근래에는 DPD와 DPV 기능을 수행할 수 있도록 확장되고 있다[2,3,4]. 그러나 아직까지 DPD/DPV프로토콜 요구조건에 적합한지 정확한 검증이 이루어지지 않은 상태이다. 본 논문에서는 OCSP가 DPD/DPV 프로토콜 요구조건을 만족하는지 IETF에서 정의한 총 23개의 기준을 적용하여 분석하고자 한다. 이와 더불어 요구조건을 만족하지 않는 기능을 보완한 개선된 OCSP (I-OCSP)를 제시하여 향후 인증서비스의 고도화를 도모하고자 한다.

2. 관련 연구

2.1 DPD/DPV 프로토콜 요구기준

본 절에서는 서버 및 클라이언트가 동작하는 일반적인 순서에 따라 DPD/DPV 프로토콜의 요구기준을 요청생성단계, 중계기능단계, 응답생성단계의 3단계로 나누고 필요한 기능을 수행해야 하는 주체에 따라 기준코드를 부여한다. 따라서 클라이언트, 서버, 프로토콜 주체별로 *C, S, P*의 기호를 사용하여 총 23개의 기준을 정의한다.

2.1.1 요청생성단계

요청생성 전처리단계로 클라이언트는 DPD/DPV서버의 인증정책 자체 또는 참조위치 등 전반적인 정보를 별도의 메시지를 이용하여 미리 획득해야 한다(*C01*). 그런 다음 클라이언트는 서버측에서 요청을 효율적으로 처리하는데 유용한 보조정보를 DPD/DPV 요청메시지를 통해 제공할 수 있어야 한다. 보조정보에는 정책 OID (Object Identifier)와 같은 인증정책관련 추가정보와(*C02*) 인증서 발급자명·인증서 해쉬값 등 처리대상 인증서 참조정보가 있다(*C03*). 또한 개별 인증서 자체정보와 관련 CRL 정보를 전달해야 하며(*C04*) 클라이언트 자신의 인증식별자정보를 제공할 수 있어야 한다(*C05*). 다음으로 서버를 절대적으로 신뢰하지 않는 제삼자가 서버의 처리결과를 믿을 수 있도록 클라이언트는 서버가 처리한 인증서 체인 및 관련 CRL 정보를 반환해 줄 것을 요청할 수 있다(*C06*). 끝으로 불완전한 시각동기화방법이 아닌 프로토콜 레벨에서 재연공격(replay attack)을 막을 수 있는 방법이 요청메시지에 존재해야 한다(*C07*).

2.1.2 중계기능단계

클라이언트의 요청을 자체적으로 처리하지 못할 경우 서버는 또 다른 서버에게 요청을 중계할 수 있는데 이러한 중계기능을 지원하기 위해 프로토콜 레벨에서 선택 또는 확장필드를 정의해야 하며(*P01*), 무한루프나 불필요한 반복수행여부를 탐지하여 이를 막을 수 있어야 한다(*P02*). 만일 서버가 다른 서버정보를 클라이언트에게 반환할 때, 클라이언트는 이를 이용하여 직접 다른 서버로 요청하는 레퍼럴(Referral)기능을 수행할 수 있어야 한다(*P03*). 또한 네트워크 구조상 침입차단시스템 또는 침입탐지시스템과 같은 제약사항을 해결하기 위한 선택적인 파라미터를 제공할 수 있어야 한다(*P04*).

2.1.3 응답생성단계

서버가 요청을 처리할 때 고려해야 할 기준으로 인증정책, 인증메커니즘, 결과코드, 결과증빙정보 등이 있다. 첫째, 인증정책 관점에서 서버는 처리대상 인증서를 포함하는 유효한 인증경로를 탐색할 수 있어야 하며(*S01*), 관련 폐지정보를 획득할 수 있어야 한다(*S02*). 이와 동시에 서버는 클라이언트가 지정한 인증정책을 적절히 처리하지 못하는 경우 에러를 반환해야 하며(*S03*), 만일 클라이언트가 인증정책을 지정하지 않는 경우, 서버에서 사용된 유효한 인증정책 정보가 반환되어야 한다(*S04*). 둘째, 인증메커니즘 기준으로 서버는 클라이언트 인증정보를 요구할 수 있으며

(S05), 서버 자신에 대한 인증정보생성을 위해 DPV 응답메시지에 반드시 전자서명 해야 한다. 그러나 DPD 응답메시지에는 필요한 경우로 제한할 수 있다*(S06)*. 셋째, 결과코드의 경우 응답은 성공 또는 실패여부를 필히 포함해야 하며*(S07)*, 만일 실패일 경우 상세한 원인을 제공해야 한다*(S08)*. 넷째, 결과증빙정보 기준으로 서버는 유효한 경로에 있는 처리대상 인증서들을 모두 획득해야 하며*(S09)*, 획득한 인증서의 직간접적인 정보를 응답메시지에 포함해야 한다*(S10)*. 또한 클라이언트가 제공하는 요청의 성격, 사유를 기술하는 텍스트 정보 또는 보조 파라미터를 응답메시지에 그대로 복사거나 해쉬값 형태로 피드백하여 요청·응답메시지 간에 연관성을 부여해야 한다*(S11)*. 기타 기준으로 DPV서버는 현재시각이 아닌 클라이언트가 요청한 임의의 시각에서의 인증서 검증을 수행할 수 있어야 한다*(S12)*.

2.2 IETF PKIX OCSP 분석

OCSP는 DPD/DPV 요구조건을 만족하기 위해 그림1과 그림3의 확장필드에 각각 그림2와 그림4의 ExtendedOCSPRequest와 ExtendedOCSPResponse 구조를 포함하여 프로토콜을 확장하였다[3]. 본 절에서는 이러한 구조가 DPD/DPV 요구기준과 부합하는지 살펴본다.

요청생성단계에서 요구되는 DPD/DPV 기능은 모두 7개이며 이 가운데 OCSP는 *C01, C02, C04*의 3개 기준을 만족하지 못한다. OCSP는 인증정책정보 획득을 위해 별도로 메시지를 정의하고 있지 않기 때문에 *C01*을 만족하지 못한다. 대부분 인증정책은 복잡한 경향이 있으며 서버의 인증정책이 클라이언트의 로컬 인증정책과 융합되어야 한다. 클라이언트가 이를 위해 요청메시지에 추가적으로 로컬 인증정책관련 파라미터를 설정할 수 있어야 *C02*를 만족하게 된다. 그러나 그림2의 initialPolicySet 필드만으로는 충분히 로컬 인증정책을 반영하기가 어렵고 관련 정보인 trustPoints와 revInfo 필드가 세부적으로 정의되어 있지 않아 해당 기준을 통과하기 어렵다. 그러나 그림1의 reqCert 필드의 사용은 *C03*기준에 적절하며 또한 그림1의 requestorName 필드를 식별자로 그림4의 reqID로 복사할 수 있으므로 *C05*를 만족한다. 그림2의 flags필드 역시 *C06*기준에 아무런 문제가 없다. 반면 불충분한 revInfo 필드와 그림4의 PathInfo나 reqContents 필드와 같은 정보가 그림2에는 없기 때문에 *C04*를 만족하지 못한다. 마지막으로 *C07*은 그림1의 requestExtension와 그림3의 responseExtension에 난수 확장필드(id-pkix-ocsp-nonce)를 사용하면 해결된다.

두드러진 사항으로 OCSP는 중계기능단계에서 요구되는 4개의 요구기준, 즉 *P01~P04*를 모두 만족하지 못한다. 이는 OCSP가 중계기능을 전혀 제공하지 못하는 데에 기인한다고 볼 수 있다.

응답생성단계에서 정의된 12개의 기준 중 OCSP는 *S03, S04, S06, S07, S08, S11*의 6개항을 만족하지 못한다. OCSP 자체적으로 인증경로 및 폐지정보를 탐색할 수 있으므로 *S01*과 *S02*를 만족한다. 그러나 인증정책을 처리하지 못하는 경우에 해당하는 사유가 그림3의 responseStatus에 없으므로 *S03* 기준을 통과할 수 없다. OCSP가 사용한 인증정책을 표현하는 그림4의 policy 필드는 상세히 정의되어 있지 않아 만일 관련 파라미터가 있을 경우 이를 클라이언트에게 전달할 방법이 없으므로 *S04*를 만족하지 못한다. 다음으로 그림1의 optinalSignature 필드의 사용은 *S05*기준과 부합하나 그림3의 signature필드는 DPD/DPV서비스에 상관없이 모두 응답메시지에 전자서명을 하게 되므로 *S06*기준에 부합하지 않는다. 동시에 *S07*과 *S08*은 그림3의 responseStatus에 정의된 결과상태코드가 일반적인 사유로 DPD/DPV에서 요구하는 상세한 상태와 그 원인을 표현하기에 부적절하다. 하지만

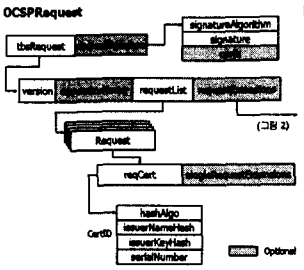

그림1 OCSPRequest

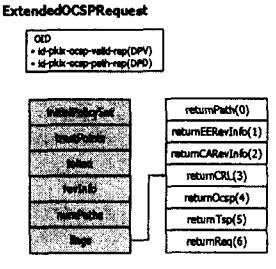

그림2 ExtendedOCSPRequest

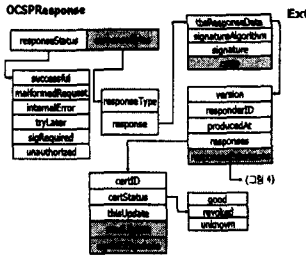

그림3 OCSPResponse

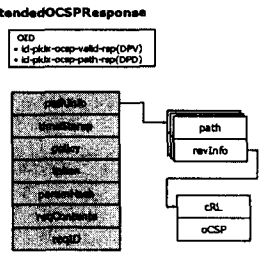

그림4 ExtendedOCSPResponse

*S09*와 *S10*은 그림3의 OCSPResponse를 통해 부합된다. *S11*은 OCTET STRING으로 정의되는 그림4의 token 필드로는 텍스트 정보를 표현하기에 부적절하므로 표현형식의 변경이 필요하다. 또한 OCSP에는 그림1과 그림2에서 임의의 시각을 표현할 수 있는 형식이 없으므로 *S12*를 만족하지 못한다.

3. 제안 방법

3.1 Improved OCSP 설계

2장에서 살펴본 바와 같이 OCSP는 DPD/DPV가 제시하는 23개의 기준 중 10개항만을 통과하며 특히 중계기능이 없는 것은 시급히 보완해야 할 사항이라고 판단된다. 이의 해결을 위해 3장에서는 문제점이 있는 것으로 드러난 상기 기준들을 만족하면서 기존 OCSP 호환성 있는 개선된 OCSP (I-OCSP)를 설계한다.

먼저 *C01*을 만족하기 위해 I-OCSP는 그림5와 같이 별도의 PolFetchRequest와 PolFetchResponse 메시지를 정의하여 어느 시점에서라도 서버의 인증정책이 클라이언트에게 제공되도록 한다. 여기서 서버의 인증정책이 RFC 3280에 정의된 인증서 경로검증 알고리즘 절차를 수행할 수 있도록 구성되어 있다고 가정한다면 클라이언트는 PolFetchResponse의 ocspPolicyOID를 통해 PathLenConstraint, acceptablePolicySet, nameConstraints, policyConstraints 등 서버에서 이용되는 여러 인증정책의 변수 상태를 파악할 수 있어 자신의 로컬인증정책에 이를 반영할 수 있다.

그림5 PolicyFetchRequest · PolicyFetchResponse 메시지

I-OCSP는 2.1.1 요청생성단계의 기준을 만족하기 위해 그림6과 같이 OCSP의 ExtendedOCSPRequest 구조를 DPD/DPV 기준에 맞도록 재설계하였다. 우선 DPD 서비스는 DPV 서비스의 일부분이므로 굳이 별도의 OID를 정의하여 혼동의 여지가 있는 OCSP에 비해 하나의 OID로 통일하여 단순명료한 서비스를 지향할 수 있도록 고려하였으며 버전(version) 정보나 서비스종류(serviceType) 필드를 두어 향후 서비스 확장에 용이하도록 구성하였다.

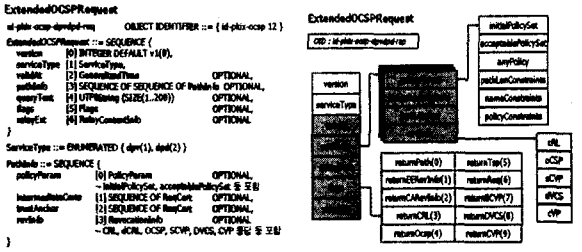

그림6 I-OCSP의 ExtendedOCSPRequest

클라이언트는 그림6의 *pathInfo*의 *policyParam* 필드를 통해 인증경로검증 변수나 인증정책과 관련된 다양한 정보를 요청메시지에 추가변수로 포함시킬 수 있다. 그리고 OCSP에서 정의가 완전하지 않았던 revInfo 필드는 CRL, OCSP, SCVP, DVCS, CVP 프로토콜 형식으로 폐지정보에 대해 다양한 정보를 수용할 수 있도록 설계되었다. 더욱이 pathInfo에는 클라이언트의 신뢰정점 역할을 하는 인증서를 비롯하여 중계인증서, 개별 인증서 관련 폐지정보를 모두 포함하는 포괄적인 구조로 결국 pathInfo는 *C02, C04, C06*기준을 동시에 만족한다. 그림6의 validAt 필드는 기준 *S12*에 부합하기 위한 필드로 I-OCSP서버는 DPV 서비스 수행시 validAt 필드에 요청된 임의의 시각에 대해서도 인증경로검증을 수행할 수 있게 된다. 또한 그림6의 queryText는 OCSP의 token 필드를 대체하는 것으로 클라이언트는 자신의 요청과 관련된 사항을 queryText안에 텍스트 정보로 표현할 수 있고 서버는 이를 다시 응답메시지에 되돌릴 수 있으므로 *S11*을 만족하는데 문제가 없다.

그림7은 클라이언트로부터 받은 요청을 처리하기 위해 서버가 또 다른 서버에게 질의할 경우의 중계기능을 위한 RelayContextInfo 구조이다. 중계기능이 필요한 경우 서버는 그림6과 그림7의 relayExt 필드에 본 구조를 사용한다. 세부적으로 doLoops 필드는 무한루프를 탐지할 수 있는 기능을 제공하며 referralFlags 필드가 서버에 의해 TRUE로 설정되는 경우 클라이언트는 serverType, serverInfo와 네트워크 제약사항을 포함하는 svrConstraints 필드정보를 이용하여 레퍼럴 기능을 수행할 수 있다. 따라서 RelayContextInfo 확장필드는 2.1.2의 중계관리와 관련된 DPD/DPV 요구기준의 *P01~P04*를 동시에 만족하는 구조로 I-OCSP는 OCSP가 지원하지 못하는 중계기능이 가능한 특징을 지닌다.

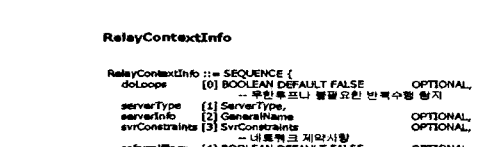

그림7 중계기능을 위한 RelayContextInfo

2.1.3의 응답생성단계의 기준을 만족하기 위해 I-OCSP의 응답메시지는 그림6의 ExtendedOCSPRequset와 유사한 형태로 그림8의 ExtendedOCSPResponse를 정의한다. *S03*을 만족시키기 위해 unsupportedPolicy 코드가 responseStaus에 추가되었다. 이외에도 partialPath, pathNotDiscovered, validationFailed등의 상태코드가 추가되어 인증정책을 적용한 DPD/DPV 서비스 결과에 대한 상세한 상태정보를 표현할 수 있게 되어 결국 *S07*및 *S08* 기준에 부합하게 된다. 또한 그림6의 pathInfo가 그대로 재사용되어 서버가 사용한 인증정책 관련정보(예를 들어 acceptablePolicySet, pathLenConstraints등)를 상세히 반환하므로 *S04*기준을 통과한다. 이외에도 pathInfo는 *S10* 기준까지 부가적으로 만족시킨다. 다음으로 그림8의 reqContents는 ExtendedOCSPRequest 메시지를 클라이언트에게 피드백하기 위한 구조로 *S11*기준을 만족하게 되는데 reqHash 필드로 무결성 정보만을 제공할 수도 있다. 끝으로 *S06*기준에 부합하기 위해 signatureAlgorithm과 signature 필드를 필수에서 선택사항으로 구성하였다. 참고로 I-OCSP는 successful 상태코드이외에도 DPD 서비스를 고려하여 *partialPath*일 경우에도 *responseBytes* 필드에 값이 채워지게 되는 구조이다.

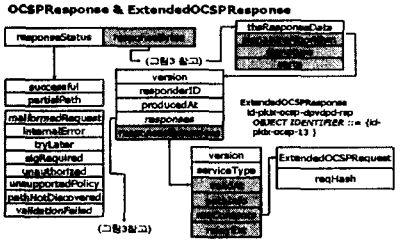

그림8 I-OCSP의 ExtendedOCSPResponse

4. 결론

본 논문에서는 OCSP가 DPD/DPV 프로토콜 요구기준에 적합한 서비스를 제공하는지 세부적인 기능에 대해 각 기준별로 살펴보고 문제점을 제시하였다. 나아가 OCSP가 지원하지 못하던 중계기능 등을 추가하여 기능을 대폭 향상시킨 I-OCSP를 제안하였다. I-OCSP는 일관성, 확장성, 유연성을 제공하는 구조로 향후 무선 인터넷 환경에서 그 중요성이 한층 부각될 DPD/DPV 프로토콜을 완전히 지원할 수 있으리라 기대된다.

5. 참고문헌

[1] D. Pinkas, R. Housley, IETF RFC 3379, Delegated Path Validation and Delegated Path Discovery Protocol Requirements, September, 2002

[2] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, IETF RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP), June, 1999

[3] M. Myers, IETF Internet Draft, DPV and DPD over OCSP(draft-ietf-pkix-ocsp-dpvdpd-00), January, 2003

[4] M.Myers, A. Malpani, D. Pinkas, IETF Internet Draft, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, version 2 (draft-ietf-pkix-ocspv2-ext-v2.01), December, 2002