대리인증경로관리 프로토콜 평가기준을 만족하는 개선된 SCVP (e-SCVP) 설계

박종욱* 이상진* 이용** 이재일**

*고려대학교 정보보호대학원

**한국정보보호진흥원 전자서명인증관리센터

A Design of the enhanced SCVP (e-SCVP) Satisfying the DPD/DPV Protocol Requirements

Jongwook Park*, Sangjin Lee*, Yong Lee** Jaeil Lee**

*Graduate School of Information Security, Korea University

**Korea Certification Authority Central, KISA(Korea Information Security Agency)

요 약

대리인증경로관리는 대리인증경로구축과 대리인증경로검증을 함께 지칭하는 개념이다. 휴대폰과 같이 한정된 컴퓨팅 파워를 갖는 클라이언트는 상대적으로 높은 계산능력이 요구되는 인증경로관리기능을 스스로 처리하지 않고 서버로 위임하여 경량화된 클라이언트를 지향할 수 있다. 본 논문에서는 대리인증경로관리 프로토콜의 하나인 SCVP에 대해 RFC 3379에서 정의한 대리인증경로관리 프로토콜 평가기준을 적용하여 그 적합성 여부를 살펴본다. 아울러 개선된 SCVP를 제안하여 평가기준을 만족하지 않는 사항을 보완하는 동시에 프로토콜의 안전성과 확장성을 증대하고자 한다.

I. 서론

근래 세계인터넷표준화기구(IETF)의 공개키기반구조(PKIX, Public Key Infrastructure based on X.509) 워킹그룹은 인증서에 대한 대리인증경로구축(DPD, Delegated Path Discovery) 및 대리인증경로검증(DPV, Delegated Path Verification) 프로토콜로 SCVP (Simple Certificate Validation Protocol)를 차세대 표준 프로토콜로 채택하였다. 이는 OCSP, SCVP, DVCS, CVP 등 다양한 후보 프로토콜 중에서 SCVP가 공식표준문서(RFC) 3379에 기술된 DPD/DPV 평가기준에 가장 근접하게 설계되었음을 반증하는 것이기도 하다[2,3,4,5]. 그러나 아직까지 정확한 SCVP 평가작업이 이루어지지 않는 상황이다. 따라서, SCVP가 차세대 표준 프로토콜로 확실히 자리매김 하기위해서는 DPD/DPV 평가기준을 완벽히 따르는지에 대한 검증작업이 선행되어야 한다. 본 논문에서는 첫째, SCVP가 대리인증경로관리 평가기준을 만족하는지를 판단하기 위하여 RFC 3379에서 제시한 평가기준을 적용하여 분석하고자 한다[1]. 또한 평가결과 문제점으로 부각된 중계기능을 지원하는 개선된 SCVP (e-SCVP)를 제안한다.

II. 대리인증경로관리 프로토콜 평가기준분석

RFC 3379에서 제시하는 평가기준은 크게 유효인증정책관리 · 대리인증경로 구축기능 · 대리인증경로검증기능 · 중계기능의 네 그룹으로 나뉜다. 본 장에서는 RFC 3379의 평가기준이 가지는 의미를 그룹내 항목별로 상세히 분석한다.

1. 인증정책

대리인증경로관리를 수행하는 서버 또는 클라이언트는 표 1에 제시된 인증정책 평가기준에 부합되어야 한다.

표 1: 인증정책 평가기준

평가코드	평가기능
P-01	유효인증정책 사전공유
P-02	인증정책관련 추가정보 공유
P-03	응답에 사용된 유효인증정책정보 명시
P-04	지원하지 않는 인증정책에 대한 에러처리
P-05	유효인증정책 적용절차
P-06	다양한 폐지정보 제공여부

P-01은 대리인증경로처리를 위한 상세한 인증

정책을 별도의 메시지를 이용하여 서버와 클라이언트가 미리 공유해야함을 의미한다. 일반적으로 인증정책은 다양한 인증서비스환경을 반영하므로 복잡한 구조로 이루어지며 새로운 환경에 따라 언제든지 추가적인 파라미터가 정의될 수 있다. 이런 경우 확장성을 제공하기 위해 서버와 클라이언트는 추가 인증정책정보를 상대방으로 전송할 수 있어야 비로소 P-02 요구사항을 만족하게 된다. 한편 클라이언트가 스스로 적절하다고 여기는 유효인증정책을 요청메시지에 지정하면 서버는 이를 이용할 수 있다. 반대로 P-03은 클라이언트가 유효인증정책을 지정하지 않을 때 적용된다. 즉, 서버가 대리인증경로처리과정에서 사용한 유효인증정책이 응답메시지에 포함되어 클라이언트에게 피드백 되는가를 살펴보는 역할을 한다. 하지만 클라이언트가 유효인증정책을 지정했음에도 불구하고 서버가 이를 적절히 처리하지 못한다면 서버는 반드시 에러를 반환해야 한다. 이는 P-04가 의도하는 목적이다. P-05를 통과하기 위해 서버는 처리대상인증서마다 최소 하나의 유효한 인증경로를 구축해야 한다. 그런 다음 RFC2459/3280을 적용하여 구축된 인증경로를 검증해야 한다. 이 때 인증정책이 폐지정보로 CRL, 델타CRL, OCSP 등을 사용한다면 P-06을 만족하게 된다.

2. 대리인증경로 구축기능

표 2는 클라이언트와 서버사이에 유효한 인증경로 구축과정이 적절히 진행되었는지를 판단할 수 있는 기준을 제시한다.

표 2: 대리인증경로 구축기능 평가기준

평가코드	평가기능
DPD-01	인증경로구축관련 추가정보 요구
DPD-02	자가서명인증서 배제
DPD-03	유효인증경로 구축여부
DPD-04	대리인증경로구축 처리결과
DPD-05	서버 및 클라이언트 인증메커니즘

클라이언트는 인증경로구축의 응답으로 단순히 인증경로상에 있는 인증서체인만을 요구하지는 않는다. 추가적으로 개별 인증서에 대한 폐지정보 혹은 상태정보를 원할 수도 있다. 따라서 요청메시지는 이러한 추가정보 요구를 포함할 수 있는 유연한 구조를 가져야 하는데 이것이 DPD-01의 요구사항이다. DPD-02를 만족하기 위해 서버는 경로구축과정에서 신뢰정점 인증서가 자가서명인증서라고 판단되면 이를 인증경로로 포함시키지 말아야 한다. 왜냐하면 자가서명인증서의 신뢰대상은 인증서 자체가 아니라 공개키이며 이는 안전하게 별도의 방법으로 획득되어야 하기 때문이다. DPD-03은 서버가 반환해준 인증경로가 클라이언트에게 유효한 인증경로가 아닐 경우 서버와 클라이언트간에 추가적인 양방향 통신메커니즘을 통해 인증경로를 재구축할 수 있는가를 평가한다. DPD-04는 대리인증경로구축에 대한 상세한 결과가 표시되는지를 살핀다. 즉 서버는 인증정책에 따라 인증경로가 구축되었는지 또는 하나이상의 인증경로는 탐색되었지만 폐지정보는 부분적으로 탐색되었는지를 결과에 나타내야 한다. 마지막으로 DPD-05는 우선 서버 및 클라이언트 개체인증방법이 존재하는지를 판단한다. 그런 후 서버가 클라이언트 인증을 수행한다면 요청메시지에 있는 클라이언트의 고유식별자를 응답메시지에 그대로 복사하여 클라이언트에게 되돌려 주는지를 평가한다. 이렇게 하면 클라이언트는 서버를 의심없이 믿을 수 있게 된다.

3. 대리인증경로 검증기능

클라이언트와 서버사이에 공유된 인증경로에 대한 대리검증처리의 정확성 여부는 표 3에서 제시하는 평가기준을 통해 결정된다.

표 3: 대리인증경로 검증기능 평가기준

평가코드	평가기능
DPV-01	임의시각에서의 대리인증경로검증처리
DPV-02	인증경로검증 대상인증서 정보공유
DPV-03	인증경로검증관련 추가정보 정보공유
DPV-04	인증경로검증 대상인증서 획득여부
DPV-05	대리인증경로검증 처리결과
DPV-06	재연공격(Reply attack) 방어메커니즘
DPV-07	경로검증결과 증빙자료 제공
DPV-08	요청/응답 메시지 연관성
DPV-09	서버 및 클라이언트 인증메커니즘

서버가 현재 시각이 아닌 클라이언트가 요청한 임의의 과거시각에서도 인증경로검증을 수행할 수 있다면 DPV-01 평가는 성공적이다. DPV-02는 서버측에 유용한 정보인 검증대상 인증서 자체나 인증서 발급자명·인증서 해쉬값 등 처리대상 인증서 간접정보가 요청메시지에 포함되는지 살펴본다. 이와 더불어 DPV-03는 검증대상인증서와 관련된 중계인증서, 폐지정보 등이 요청메시지에 포함되는지 평가한다. DPV-02,03의 결과로 서버는 처리한 검증대상 인증서에 대한 직·간접적인 인증서 정보를 응답메시지에 명기해야 DPV-04를 통과하게 된다. DPD-04와 마찬가지로 서버가 DPV-05에 적합하려면 상세한 결과를 응답메시지에 표시해야 한다. 참고로 결과는 응답메시지 전체와 개별인증서에 대한 검증결과로 구분되어진다. 그리고 주목할 만한 사항으로 클라이언트 인증은 선택사항이므로 서버는 재연공격(replay attack)에 취약할 수밖에 없다는 것이다. 따라서, DPV-06은 불완전한 시각동기화방법이 아닌 프로토콜 레벨에서 재연공격을 막을 수 있는 메커니즘이 존재하는지 조사한다. DPV-07은 인증경로 검증에 사용된 인증서체인, 폐지정보 등을 클라이

언트에게 피드백함으로써 서버측에서 인증서 경로 검증이 정확히 되었다는 것을 보장하기 위한 일종의 안전장치다. 참고로 서버는 요청메시지를 응답메시지내에 해쉬값형태로 제공할 수 있다. DPV-08은 요청·응답메시지간에 연관성이 있는가를 판단한다. 이를 위해 서버는 클라이언트측이 제공하는 요청의 성격, 사유를 기술하는 텍스트 정보 또는 보조 파라미터를 응답메시지에 그대로 복사거나 해쉬값 형태로 포함해야 한다. 마지막으로 DPV-09는 근본적으로 DPD-05와 동일한 목적을 갖는 평가기준이다.

4. 중계기능 기준

DPD/DPV서버는 클라이언트의 요청을 직접 처리하지 못하는 경우 다른 OCSP, SCVP, DVCS, CVP 서버 등에게 대신 처리해줄 것을 요청한다. 이런 메커니즘을 중계기능이라 하며 인증서비스의 가용성을 보장한다. 중계기능 평가기준은 표 4와 같다.

표 4: 중계기능 평가기준

평가코드	평가기능
R-01	중계기능관련 추가정보 공유
R-02	무한루프나 반복수행 탐지 메커니즘
R-03	클라이언트의 레퍼럴(Referral) 수행능력
R-04	네트워크관련 추가정보 처리능력

사실 DPD/DPV 프로토콜은 중계기능을 반드시 지원할 필요는 없다. 그러나 중계기능을 제공하는 것은 인증서비스의 가용성과 확장성을 고려할 때 상당히 바람직한 방향이다. 중계기능을 제공하기 위해 서버 및 클라이언트는 R-01이 요구하는 바와 같이 메시지내 선택 또는 확장필드를 통해 중계처리에 필요한 정보를 포함해야 한다. 본질적으로 중계기능은 복잡한 네트워크 경로구조상 자칫 무한루프나 반복수행 될 위험이 크므로 R-02에서 명시하듯이 원치 않는 상황이 발생할 경우를 탐지해 낼 수 있는 메커니즘이 프로토콜 차원에서 반드시 지원되어야 한다. 어떤 특정한 환경에서는 서버가 다른 서버의 정보만을 클라이언트에게 전달하고 클라이언트는 이를 이용하여 직접 다른 서버로 재차 연결할 수 있는 상황을 고려할 수 있다. 클라이언트가 이러한 '레퍼럴' 기능이 있는지는 R-03을 통해 평가된다. 중계기능을 이용하여 다른 서버가 물리적으로 방화벽, IDS, ESM 등으로 보호된 네트워크에 위치하여 액세스가 용이하지 않는 경우가 발생할 수 있다. R-04는 상기와 같은 네트워크 제약사항에 대한 정보가 요청메시지의 선택필드로 제공되어 서비스의 가용성을 보장하는지 평가한다.

III. SCVP 분석

1. SCVP 개요

SCVP는 중앙집중적인 인증정책관리를 근간으로 인증서 처리를 클라이언트 대신 서버에게 위임하는 2개의 Request-Response 모델을 사용한다. 첫째는 대리인증경로처리기능을 수행하고, 둘째는 서버와 클라이언트간에 인증정책공유를 목적으로 한다. 대리인증경로처리를 위한 Request는 하나 이상의 인증서 정보와 관련 보조정보를 포함한다. 그리고 Response는 인증경로 구축 또는 검증결과와 추가정보 등을 포함한다. 한편 인증정책공유는 인증정책에 대한 대표성을 의미하는 오브젝트식별자(OID, Object Identifier)를 서로 공유하는 것을 목적으로 한다. 특이사항으로 SCVP는 클라이언트에게 2가지 모드로 동작한다는 것이다. 비신뢰된 SCVP와 신뢰된 SCVP가 바로 그것인데, 비신뢰된 SCVP 서버는 클라이언트가 직접 인증서 경로검증을 수행할 때 필요한 인증경로와 관련된 폐지정보만을 제공하는데 비해 신뢰된 SCVP 서버는 완전하게 대리인증경로검증을 통해 클라이언트 대신 인증서 검증을 수행한다.

2. SCVP 적합성 평가

SCVP는 본 논문에서 제시한 총 24개의 평가기준 중 표 5에서 볼 수 있듯이 15개 기준을 만족한다. 그러나 중계기능 지원부재를 비롯하여 인증정책·대리인증경로 검증기능 등 평가부분에서 총 9개 항목은 부적합하거나 개선의 여지가 있는 것으로 나타났다.

표 5: SCVP 적합성 평가결과 요약

구분	적합	일부적합	부적합
인증정책	P-02 P-03 P-04 P-05 P-06	P-01	
대리인증경로 구축기능	DPD-01 DPD-02 DPD-03 DPD-04	DPD-05	
대리인증경로 검증기능	DPV-01 DPV-02 DPV-03 DPV-05 DPV-06 DPV-07	DPV-04 DPV-09	DPV-08
중계기능			R-01 R-02 R-03 R-04
총계	15	4	5

1) 인증정책

SCVP서버는 인증정책공유를 위한 VPRequest와 VPResponse 메시지를 표 6과 같이 별도로 정의하고

있다. 그러나 인증정책에 대한 상세한 내용이 아니라 오브젝트 식별자만이 공유되므로 P-01에 적합하기 위해서는 상세한 정보를 포함할 수 있는 구조로 확장되어야 한다.

표 6: SCVP 인증정책공유 메시지

```
-- 요청메시지
VPRequest ::= SEQUENCE {
  scvpVersion     INTEGER }

-- VPResponse (응답메시지)
ValPoliciesResponse ::= SEQUENCE {
  scvpVersion     INTEGER,
  valPolicies     SEQUENCE OF OBJECT IDENTIFIER }

id-svp-defaultValPolicy OBJECT IDENTIFIER ::=
                                { id-svp 1 }
```

P-02는 서버와 클라이언트 모두 그림 1,2의 parameters를 갖는 valPolicy을 사용하므로 문제없다. 그림 2의 valPolicy는 서버의 인증정책을 나타내므로 P-03을 만족한다. 그리고 그림 2의 unrecognized-ValPolicy의 사용은 클라이언트가 요청한 인증정책을 서버가 처리하지 못하는 경우의 결과값으로 P-04 역시 평가기준을 통과하게 된다. SCVP는 RFC2459/3280에 따른 인증경로처리를 기반으로 하고 있으므로 P-05적용에도 무리가 없다. CRL, 델타CRL, OCSP 등 폐지정보는 그림 1의 revocationInfos와 그림 2의 replyWantBacks를 통해 사용되므로 P-06을 만족하게 된다.

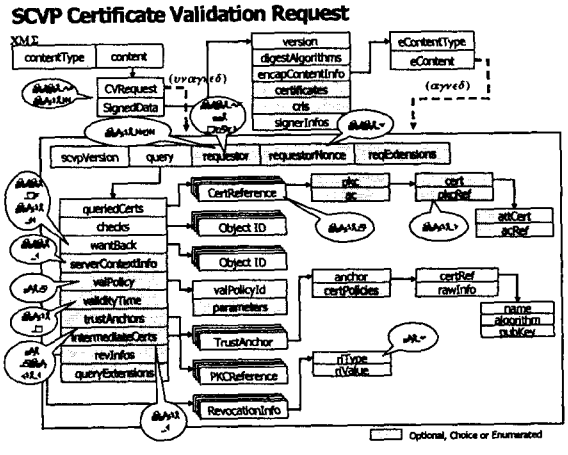

그림 1: SCVP 요청메시지 도식도

2) 대리인증경로구축 기능

클라이언트는 그림 1의 wantBack을 통해 원하는 인증경로, 폐지정보 등을 서버에 요구할 수 있으므로 DPD-01를 만족한다. 그리고 SCVP서버는 자가서명인증서가 그림 2의 replyWantBacks에 포함하는 것을 배제하므로 DPD-02 역시 만족한다. 다음으로 그림 1,2의 serverContextInfo는 클라이언트와 서버간의 경로구축을 위한 상호작용의 매개체로 작동한다. 즉, 클라이언트는 최종적으로 유효한 인증경로를 획득할 수 있어 DPD-03을 문제없이 통과하게 된다. DPD-04의 경우 그림 2의 responseStatus · replyStatus · replyChecks · replyWantBacks가 인증경로구축의 결과를 상세히 나타내므로 요구하는 평가기준을 만족한다. SCVP는 그림1,2와 같이 서명된 SignedData나 서명되지 않는 일반데이터를 사용하여 개체인증을 선택적으로 지원한다. 중요한 것은 클라이언트의 인증이 수행될 때, 클라이언트 식별자로 requestor를 사용한다는 것이다. 그러나 requestor는 대리인증경로검증 및 중계기능을 위한 요소로도 사용된다. 이러한 사용목적의 중복은 원래의 기능을 수행하는데 위험요소로 작용하므로 수정되어야 한다.

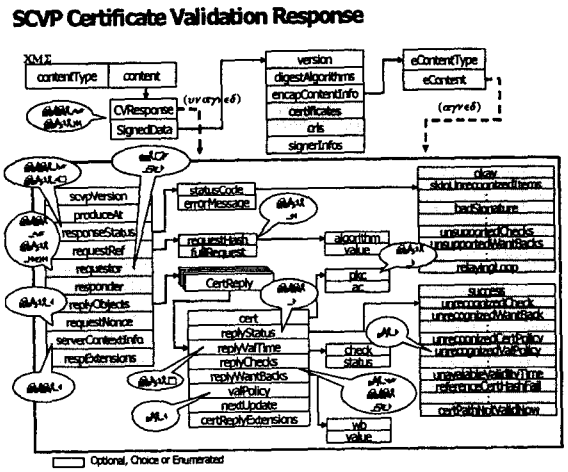

그림 2: SCVP 요청메시지 도식도

3) 대리인증경로검증 기능

클라이언트는 그림 1의 validityTime을 이용해 임의의 시각을 지정할 수 있다. 또한 서버는 그림 2의 replyTime을 통해 해당시각정보를 반환하므로 SCVP는 DPV-01을 만족한다. 또한 클라이언트는 queriedCerts를 통해 검증대상 인증서 자체를 포함하거나 간접적으로 ESSCertID를 통해 인증서 참조정보를 서버에게 전달할 수 있다. 따라서 SCVP는 DPV-02를 만족한다. 그림 1의 trustAnchors, imtermediateCerts, revInfos는 각각 신뢰정점 인증서, 중계인증서, 폐지정보 등 인증경로검증에 유용한 추가정보를 제공하므로 SCVP는 DPV-03을 문제없이 지원한다. 그러나 SCVP는 DPV-04를 수용하기 위해 수정이 불가피하다. 즉, 클라이언트는 그림 1에서 보듯이 certs나 pkcRef를 이용해 인증서의 직 · 간접정보를 선택해서 보낼 수 있다.하지만, 서

버는 그림 2의 cert필드에 처리대상 인증서의 자체정보만을 넣을 수 있는 구조이다. 따라서 이러한 비대칭구조는 클라이언트가 간접정보로 인증서에 대한 해쉬값만 보낸 경우에도 서버는 항상 인증서 자체를 보내게 한다. 결국 클라이언트에서 한번 해쉬 연산을 해야 하므로 클라이언트에게는 부담으로 작용된다. DPV-05는 DPD-04와 동일한 조건으로 만족되며 SCVP는 재연공격을 탐지해 내는 매개체로 requestNonce를 사용하므로 DPV-06 또한 문제없이 수용할 수 있다. 클라이언트는 그림 1의 wantBack를 통해 인증경로 및 폐지정보에 대한 추가정보를 요청할 수 있으며 서버는 그림 2의 requestRef를 통해 요청메시지 전문 또는 해쉬값을 되돌릴수 있으므로 DPV-07을 만족한다. SCVP는 requestor를 통해 요청의 성격, 사유 등 보조정보를 전달하고자 하나 본질적으로 텍스트필드이어야 하므로 OCTET STRING으로 표현되는 requestor필드의 사용은 DPV-08를 만족하는데 실패하게 된다. 더구나 앞서 언급한 바와 같이 requestor를 여러 목적으로 사용하는 것은 바람직하지 않다. DPV-09는 DPD-05와 동일하게 개선이 필요한 부분이다.

4) 중계기능

중계기능은 대리인증경로관리 프로토콜의 선택사항이다. 그러나 SCVP는 OCSP과는 달리 중계기능을 일부 고려하였으나 상당부분 미흡하다[6]. 특히 SCVP는 requestor을 DPD-05, DPV-08,09와 함께 R-01,02,04를 지원할 목적으로 재사용하고 있어 실질적으로 중계기능을 수행할 수 있는 능력이 있다고 볼 수 없다. 따라서 중계기능 및 레퍼럴 기능을 위한 새로운 메커니즘이 필요하다.

IV. e-SCVP 설계

본 장에서는 Ⅲ장에서 문제점이 있는 것으로 드러난 9개 평가항목을 보완한 e-SCVP를 설계한다. 제안하는 e-SCVP는 중계기능을 비롯하여 확장된 정책관리 기능과 강화된 DPD/DPV 기능을 프로토콜 차원에서 제공한다.

1. 정책관리 프로토콜 확장

e-SCVP의 확장된 정책관리 프로토콜은 표 7과 같다. 일반적으로 클라이언트는 자신만의 로컬인증정책을 관리할 수 있다. 서버와 인증정책에 대한 정보를 공유하는 것은 마치 SSL암호채널 형성과정과 비슷하다. 즉, SSL클라이언트와 SSL서버간에 CipherSuite 정보를 교환하듯이 클라이언트는 localValPolicies를 통해 자신이 유효하다고 판단하는 인증정책의 OID와 추가파라미터 집합을 서버에게 보낸다. 여기서, 추가파라미터는 PathLenConstraints, acceptablePolicySet, nameConstraints, policyConstraints 등과 같이 RFC2459/3280을 준용한 인증경로검증시 중요한 변수역할을 하는 것들을 포함할 수 있다. 그런 다음 서버는 자신이 가지고 있는 인증정책집합들과 클라이언트가 보낸 인증정책집합과의 비교를 통해 최종적으로 적용할 인증정책을 valPolicies에 담아 클라이언트에 보내준다. 여기서 valPolicies와 DefaultPolicies는 기존 SCVP에 정의되어 있는 것이지만 추가 파라미터를 수용할 수 있도록 ValidationPolicy을 적용하여 확장된 구조이다. 결론적으로 e-SCVP는 P-01을 완전하게 만족하며 중앙집중적으로 운영되는 서버의 유효인증정책과 클라이언트의 로컬인증정책이 일치가 되도록 한다.

표 7: e-SCVP 인증정책공유 메시지

```
VPRequest ::= SEQUENCE {
  scvpVersion      INTEGER DEFAULT v1(0),
  localValPolicies  SEQUENCE SIZE (0..MAX) OF
                    ValidationPolicy }

ValidationPolicy ::= SEQUENCE {
  valPolicyId      OBJECT IDENTIFIER,
  parameters       ANY DEFINED BY valPolicyId OPTIONAL }

-- VPResponse
ValPoliciesResponse ::= SEQUENCE {
  scvpVersion      INTEGER DEFAULT v1(0),
  valPolicies      SEQUENCE SIZE (1..MAX) OF
                    ValidationPolicy }

DefaultPolicy ::= ValidationPolicy — DefaultPolicy 재정의
```

2. 중계기능 구현

e-SCVP으 두드러진 차이점은 SCVP와 다르게 중계기능을 지원한다는 것이다. 표 8은 클라이언트로부터 받은 요청을 서버가 또 다른 서버에게 중계할 수 있도록 RelayContextInfo 구조를 정의한다. 물론 상기 구조는 클라이언트가 레퍼럴을 수행할 수 있도록 다른 서버의 정보를 클라이언트에게 전달하는 목적으로도 이용된다. 중계기능이 필요한 경우 서버는 그림 3의 reqExtensions이나 그림 4의 respExtensions에 RelayContextInfo를 포함시킨다. 세부적으로 살펴보면 loopInfo는 무한루프를 탐지할 수 있는 기능을 제공한다. reqHash는 요청메시지의 해쉬값으로 만일 동일한 값들이 송신자에게 되돌아오면 반복수행임을 알 수 있다. 이때 checkLoops는 TRUE로 설정되고 멀티캐스팅으로 네트워크상에 해당 서버들에게 알린다. 만일 클라이언트가 레퍼럴기능을 필요로 한다면, 서버는 ReferralInfo를 클라이언트에게 제공한다. 이때 doReferral은 TRUE로 설정된다. 다음으로 클라이언트는 svrType, svrRef를 이용해 인증경로처

리를 요청할 다른 서버에게로 접근을 시도한다. 라우팅 수행시 방화벽, IDS, ESM 등 네트워크 보안장비에게 자신을 인증하기 위해 svrConstraints에 포함된 추가정보를 이용한다. 이렇듯 여러 가능한 상황을 고려하여 구성된 RelayContextInfo 확장필드는 중계관리 평가기준인 R-01~04를 동시에 모두 만족하는 구조이다. 따라서, e-OCSP는 SCVP가 지원하지 못하는 중계기능을 완벽하게 제공하는 차별성을 가진다.

표 8: e-SCVP 중계기능 메시지

```
RelayContextInfo ::= SEQUENCE {
  loopInfo     LoopInfo OPTIONAL,
  referralInfo  ReferralInfo OPTIONAL }

LoopInfo ::= SEQUENCE {
  checkLoops    BOOLEAN DEFAULT FALSE OPTIONAL,
  reqHash       requestHash -- (그림 1) 참고 }

ReferralInfo ::= SEQUENCE {
  doReferral     BOOLEAN DEFAULT FALSE OPTIONAL,
  svrType        ServerType OPTIONAL,
  svrRef         GeneralNames OPTIONAL,
  svrConstraints ServerConstraints OPTIONAL }

ServerType ::= ENUMERATED
                    { ocsp(1), scvp(2), dvcs(3), cvp(4) }

ServerConstraints ::= SEQUENCE SIZE (1..MAX)
                        OF AttributeTypeAndValue
```

3. DPD/DPV 기능강화

e-SCVP는 동일한 목적을 갖는 DPD-05와 DPV-09를 동시에 만족시키기 위해 그림 3과 그림 4의 requestor를 사용한다. SCVP는 requestor를 여러 가지 목적으로 사용하고 있으나 e-SCVP는 단 한가지의 목적만으로 사용하여 애매모호함을 제거하였다. 다시 말하면, e-SCVP는 requestor를 클라이언트의 식별자로 간주하여 요청메시지에 포함시킨 후 서버가 이를 응답메시지로 복사할 수 있도록 하고 있다. 따라서, 클라이언트는 응답메시지의 requestor를 통해 서버가 믿을만한 주체라고 인식하게 된다. e-SCVP는 DPV-04를 만족하기 위해 그림 4와 같이 cert를 인증서 직접정보인 fullCert와 간접정보인 certHash로 구분하였다. 따라서, 클라이언트는 보내준 인증서에 대한 별도의 해쉬값을 구하는 추가연산 없이 서버가 보낸 인증서의 해쉬값과 certHash를 직접 비교하여 각자 공유한 검증대상인증서가 동일한지 판단할 수 있게 된다. 다음으로 e-SCVP는 DPV-08을 만족하기 위해 SCVP의 requestore대신에 그림 3의 reqExtensions과 그림 4의 respExtensions에 UTF8String으로 표현되는 queryText를 추가 정의한다. 결국 e-SCVP는 요청의 성격, 사유 등 보조 텍스트 정보를 그대로 변형없이 응답에 되돌릴 수 있어 요청과 응답사이에 연관성이 부여될 수 있다.

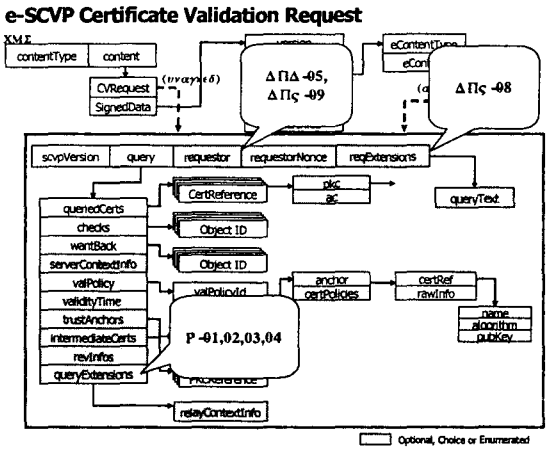

그림 3: e-SCVP의 요청메시지 도식도

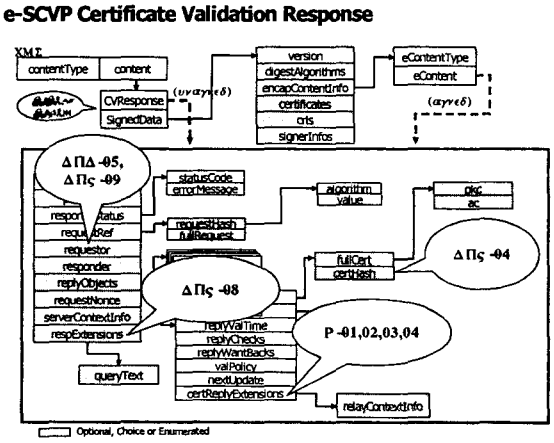

그림 4: e-SCVP의 요청메시지 도식도

V. 결론

본 논문에서는 DPD/DPV를 함께 일컫는 대리인증경로관리 프로토콜 평가기준에 SCVP가 적합한지를 분석하였다. 즉, 인증정책관리, 대리인증경로구축, 대리인증경로검증, 중계기능별 기능에 대한 상세한 평가를 통해 총 24개 기준 중 9개 기준이 부적합함을 제시하였다. 나아가 SCVP가 지원하지 못하던 중계기능을 비롯하여 인증정책관리기능 등을 대폭 향상시킨 e-SCVP를 제안하였다. e-SCVP는 확장성 및 가용성을 강조한 프로토콜로 도래하는 무선 인터넷 환경에서 그 중요성이 한층 부각될 대리인증경로관리 프로토콜을 완전히 지원할 수 있으리라 기대된다.

참고문헌

[1] D. Pinkas, R. Housley, *"Delegated Path*

Validation and Delegated Path Discovery Protocol Requirements", IETF, RFC 3379, September, 2002

[2] A.Malpani, R. Housley, T. Freeman, *"Simple Certificate Validation Protocol (SCVP)"*, IETF, draft-ietf-pkix-scvp-11.txt, December, 2002

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

[4] C. Adams, P. Sylvester, M. Zolotarev, R. Zuccherato *"Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols"*, IETF RFC 3029, February, 2001

[5] D. Pincas, *"Certificate Validation Protocol"*, IETF, draft-ietf-pkix-cvp-02.txt, January, 2003

[6] 박종욱, 서정훈, 이용, 이재일, "DPD/DPV 프로토콜 요구기준을 만족하는 개선된 OCSP (I-OCSP) 설계", 한국정보처리학회 춘계학술발표대회논문집, 2003년 4월