무선환경에서 안전한 WPKI Protocol의 설계 및 구현

- Design and Implementation of the secure WPKI Protocol on mobile environment -

장 유 진 *
Jang Yu Jin
박 상 민 **
Park Sang Min
신 승 호 ***
Shin Seung Ho

Abstract

The existing PKI authentication structure uses the OCSP method. The primary task of OCSP is to verify the status of a transaction after verifying the validity of the certificate; but, because of continuing policy changes and updates within the PKI authentication method, the status of certificates and the structures are not consistent. Therefore, the SCVP method can be selected as the broadest method for completing authentication tasks accurately because the SCVP method includes validation of policy changes. An appropriate method for building an mobile environment within the capabilities of low-memory and reduced processing CPU needs to be assessed and developed. This thesis proposes a verification method that is independent of platform and applicable to any OS in building and expanding the mobile environment.

Keyword : WPKI, OCSP, SCVP

1. 서 론

인터넷은 정보 공유의 측면뿐만 아니라 경제, 사회, 분야를 망라한 모든 분야에서 많은 응용 분야를 발생시켜 생활의 중요수단으로 자리 잡고 있다. 이러한 인터넷과 무선

† 본 연구는 과학기술부 지정 동북아전자물류연구센터의 지원 및 2003년도 인천대학교 교내 연구비 일부 지원에 의한 것입니다

* 인천대학교 컴퓨터공학과 석사과정
** 현재 인천대학교 산업공학과 교수로 재직 중
***현재 인천대학교 컴퓨터공학과 교수로 재직 중

이동 통신의 결합으로 휴대전화를 통한 무선 인터넷사용이 급격히 늘어나고 있는 실정이다. 전자 상거래의 안전성 보장을 위해 가장 필요한 것은 전자상거래 시에 교환되는 전자 문서에 대한 정보 보호이다. 전자상거래의거래 규모는 해마다 지속적인 성장을 이루어 왔으며, 현재 도입 단계에 있는 이동 통신 단말기를 이용한 새로운 이동 환경의 등장으로 인해, 향후 5년에서 10년 사이에 또 한번 놀랄만한 전자 상거래의 변화와 성장을 이룰 것으로 예상 되고 있다. 보안상의 인증 및 정보보호 등에 관한 거래 장소가 쉽게 노출되는 가상의 공간에서 이루어지고, 네트워크를 공유하는 제 3자에게 거래 내용이 노출되며, 서버의 보안상의 취약점이나 내부관련자에 의한 비밀 정보의 유출의 위험이 있고, 사용자가 직접 금융 시스템으로부터 인증을 받을 수 없고, 지불시스템을 통하여 연결되기 때문에 지불 시스템의 내부 관리자에 의한 정보 유출의 위험이 있다. 그리하여 본 연구에서는 WPKI(Wireless Public Key Infrastructure)를 이용하여 현재 이용되어지고 있는 기존의 보안을 강화한 WPKI를 구현하려 한다.

2. 관련연구

2.1 PKI (Public Key Infrastructure)

PKI는 인증서 기반 공개키 암호 시스템의 구현 및 운영을 지원하기 위해 다음과 같은 객체들로 구성한다.

① Digital 인증서를 발급하고 검증하는 인증기관(CA: Certificate Authority)
② 공개키 또는 공개키에 관한 정보를 포함하고 있는 인증서(Digital Certificate)
③ Digital 인증서가 신청자에게 발급되기 전에 인증기관의 입증을 대행하는 등록기관 (RA: Registration Authority)
④ 공개키를 가진 인증서들 이 보관 되고 있는 하나 이상의 Directory (Directory Server)
⑤ 인증서 관리 시스템

2.2 인증서의 유효기간

유무선 공개키 기반 구조간의 제일 큰 차이점은 인증서를 검증하는데 있다. 일반적으로 PKI기반의 공개키 암호 시스템을 사용함에 있어서 클라이언트가 가지는 컴퓨터 부하는 상대방의 인증서를 검증하는데 많이 걸린다. 이러한 검증단계는 사용자가 신뢰할 수 있는 인증기관이 서명한 것인지 인증서에 포함된 인증기관의 서명이 올바른지 검사하고, 인증서의 사용용도가 현재 작업에 적합한지와 인증서의 유효 기간 등을 검사해야만 한다. 여기서 가장 문제가 되는 부분이 인증서의 유효기간을 검증하는 것이다. 일반적으로 인증기관으로부터 발급 받는 사용자 인증서는 1년 정도의 유효 기간을 갖지만 사용자가 비밀키를 저장하고 있던 Hard Disk가 Format되거나 Smartcard/USB키

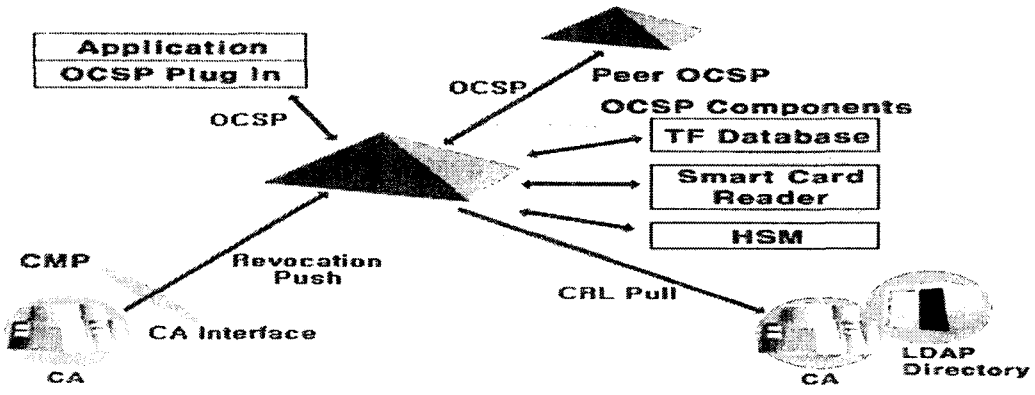
를 분실한 경우 등과 같이 인증서의 유효기간이 만료 되기 전에 인증서를 폐지하여야 만 하는 경우가 발생할 수 있다. 이로 인해 인증기관들은 유효기간이 만료되기 이전에 폐지된 인증서들의 목록(인증서 폐지 목록: Certificate Revocation List: CRL)을 유지해야만 하고, 이를 주기적으로 갱신하여야 한다. 인증서 검증단계에서 모든 단계가 성공한다 하더라도 해당 인증서가 CRL에 등록 되어 있는지를 검사하는 것은 필수 사항이다. 이러한 작업을 수행하기 위해서는 클라이언트에 인증서를 검증할 정보들이 필요하다. 유선 환경에서는 클라이언트가 디렉토리 서버로부터 인증서 폐지 목록을 주기적으로 Download해서 사용하지만 무선 환경에서는 제한된 컴퓨터 Power와 메모리를 가지고 있으며, 주기적으로 CRL을 Download하기 위해 소요되는 시간과 비용으로 인해 사실상 적용이 불가능하다. 이러한 문제를 해결하기 위해서 제안된 방법이 Short Lived Certificate를 이용하거나 실시간으로 인증서의 상태를 검증요청(OCSP: Online Certificate Status Protocol)하는 인증서 검증 방법이다.

2.3 보안 프로토콜

1) OCSP (Online Certificate Status Protocol)

공개키 기반구조 내에서 인증서에 대한 상태 정보를 알기 위해 서버에게 문의하는데 사용되는 프로토콜로서, 인증서 상태 정보를 요구하는 질의 메시지와 인증서 상태정보 요구에 응하는 응답 메시지로 구성된다.

특정 인증서의 취소상태를 시기적절하게 제공하기위한 절차이다. OCSP는 그림 1과 같이 OCSP 서버와 OCSP 클라이언트간에 수행된다. OCSP 클라이언트는 특정 인증서의 유효성과 취소상태를 서버로 문의하고, 서버는 인증서 유효성과 취소상태를 전달한다. 클라이언트는 서버로부터 인증서가 유효하고 취소되지 않았다는 정보를 수신한 후에 수신된 인증서를 사용해야 된다. OCSP규격에서는 서버와 클라이언트의 기능과 인증서의 상태를 확인하기 위하여 교환해야 하는 데이터형태로 정의된다. 이는 실시간으로 인증서의 유효상태를 확인할 수 있는 장점이 있다.



< 그림 1 > OCSP 구성 요소

2) SCVP (Simple Certificate Validation Protocol)

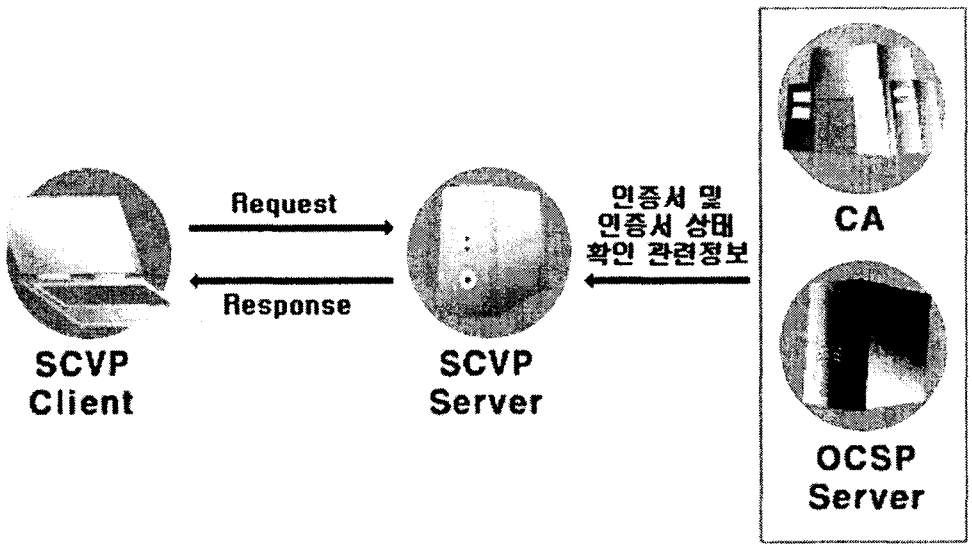
SCVP는 클라이언트가 인증서 다루는 것을 서버에서 다루도록 하는 것을 허용한다. 서버는 인증서가 유효한지, 인증서 경로를 신용장치와 폐지상태와 같은 인증서에 대해서 가치 있는 정보의 다양성을 클라이언트에게 제공한다. SCVP는 클라이언트가 수행하는 것을 간단히 하고, 회사들이 신용과 정책 경영을 중앙 집중화 하는 것을 허용하는 것을 포함하는 많은 목적들을 가졌다.

SCVP(단순 인증서 검증 프로토콜)는 그림 2와 같이 SCVP 서버와 고객간의 프로토콜로서 서버는 인증서 유효성에 관한 정보와 믿을 수 있는 인증서까지의 인증서 경로 유효성 등의 다양한 정보를 클라이언트에게 제공한다.

2003년의 인터넷 국제 표준화 기구(IETF: Internet Engineering Task Force)는 미국의 California주의 San Francisco에서 56번째 회의에서, DPD/DPV 표준 프로토콜로 SCVP를 선택하였다.

이 조사에 나타난 기본 조건은 프로토콜이 반드시 수행하는 사람들 중에서 적당한 지원이 있어야 하고, 반드시 RFC 3379에 있는 요구사항을 만족하여야 하며, 향후 완성을 위하여 충분히 조건이 만들어져야 한다.

인증서 확인은 복잡한 과정이다. 만일 PKI가 업무와 환경의 다양함에서 광범위하게 전개되어진다면, 인증서 확인은 많은 처리 시간이 걸린다. 그래서 이것은 복잡한일이고, 보다 넓고 응용들의 다양성과 보다 많은 환경 안에서 인증서확인을 완성하는 것이다. 인증서 처리시간은 감소되거나 간단하게 되는 것이 필요하다. 즉 다시 말하면, 인증서 확인의 복잡성은 많은 응용들과 환경 속에서 성공적으로 처리되는 것을 방해하지만, 인증서 확인은 많은 보안 직무들을 처리하기 위해서 필요하다.



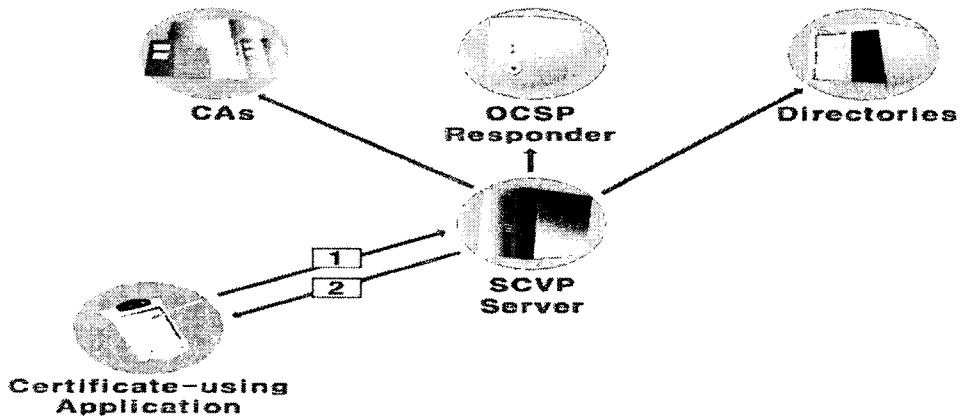
< 그림 2 > SCVP 구성도(1)

공개키 인증서를 사용하게 할 수 있는 응용들의 다양함 들이 있지만, 이 응용들은 인증서 경로들을 만들고, 유효화 하는 비용으로 부담되어진다.
인증서 확인에는 3가지 필수 단계가 있다.

1. Certificate Path Building
   인증서들의 경로를 만든다.
2. Certificate Path Verification
   경로에 있는 각 인증서의 다른 내부 field들과 서명들이 유효하다고 확인한다.
3. Certificate Status Checking
   인증 경로에서 각 인증서는 그것의 발행자에 의해서 아직 폐지되지 않았는지 확실해야 한다.

SCVP 서버는 위의 3가지 단계를 모두 취함으로써, 인증서를 사용하는 응용을 위해 이 비용은 감소되도록 설계되었다. 이제 인증서를 사용하는 응용들은 단지 SCVP Validation Authority에 의도된 목적으로 신뢰(trustworthy) 할 수 있도록 고려 될 수 있는지를 물을 수 있다.

모든 검사가 SCVP에 위임된 것과 같다. 그래서 그것은 이동 단말기나 PDA들과 같은 단말기들에 있는 메모리공간을 늘려야 한다. 응용을 위한 PKI-발자국(PKI-footprint)은 데이터를 처리하기 위해서는 필요한 메모리크기를 확장 시켜야 한다.
SCVP는 또한 각 고객 Application 안에 있는 그것들을 수행하기 보다는 한 조직 안에서 PKI 정책의 중앙 관리와 집행을 허용한다. 그것은 또한 PKI 접근들을 인증서 사용 Application들로부터 방어한다. 다시 말하면, 그것은 Upgrading이 서버 Level에서 이루어져서 그 서버는 클라이언트 level(Mobile level)에 보다 진일보한 것에 적응할 수 있는 것을 제안한다. 그것이 나중에 변화가 있는 것을 허용하기 때문에, 이것이 Future-proof라고 불리어진다. Back-end 변화는 Mobile 클라이언트에 영향을 미치지 않고 Mobile 클라이언트가 갱신을 하지 않거나 보다 새로운 기술 사용자가 또한 성공적으로 그 인증기관 처리를 허용하는 것을 만든다.[5]



< 그림 3 > SCVP 구성도(2)

그림 3은 SCVP 서버가 작동하는 것을 보여준다. 그리고 SCVP의 특징을 알아보면 다음과 같다.

Application을 사용하는 인증서는 SCVP 서버에게 인증 경로를 인증기관에 요구(Request)(1)을 할 수 있고, 그 경로를 확인하고 그 경로에 있는 각 인증서 폐지 상태를 검사할 수 있다.

Application을 사용하는 인증서는 요구(Request)(1) 안에서 또한 이것이 SCVP 서버가 돌려보내는 것을 원한다는 것이 같은 것인지를 확인할 것이다. 전통적으로 이것은 의도된 목적을 위한 인증서의 전체적인 신뢰 상태이다.

SCVP 서버가 요구(Request)를 받을 때, 다음 절차로 진행된다.

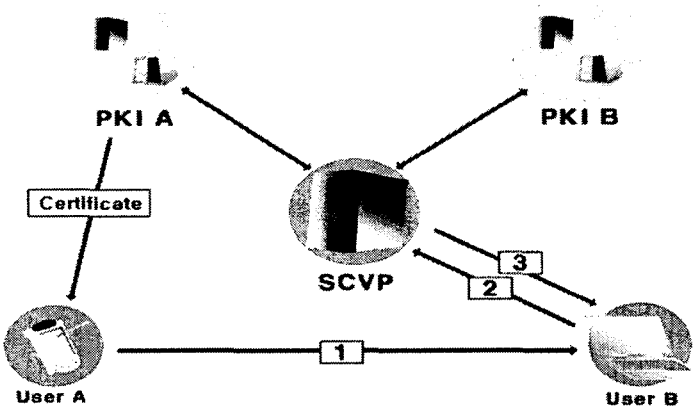
(가) 인증서 사슬은 인증 기관에 만든다. 그것은 관련된 인증서를 back-end LDAP 디렉토리에서 검색하고, Root 인증기관에 사슬을 만들 수 있는지를 검사하게 된다.

만일 이 단계에서 실패하면, SCVP는 정해진 것에 따라 그 인증서는 "not valid"라고 그 Application을 사용하는 인증서는 응답할 것이다.

(나) 만일 (가)단계를 성공적으로 지나면, SCVP는 경로에 있는 각 인증서를 지역적으로 검증하게 된다. 그것은 각 인증서에 있는 서명을 대조할 것이며, 각 인증서에 있는 날짜의 유효성을 대조하며, 그것은 인증서안에 있는 모든 인식할 수 있는 확장자들이 유효하여야 된다.

만일 이 단계에서 실패하면, SCVP는 정해진 것에 따라 그 인증서는 "not valid(인증되지 않음)"이라고 그 Application을 사용하는 인증서는 응답할 것이다.

(다) 만일 (나)단계를 성공적으로 지나면, SCVP는 그 경로에 있는 각 인증서의 폐지 상태를 조회할 것이다. 그것은 실시간 OCSP 응답기를 교신하거나, 관련된 디렉토리로부터 적당한 CRL을 검색하게 된다. 만일 그 경로에 있는 모든 인증서들 이 여전히 옳다고(예를 들어 폐지되지 않았다거나) 여겨지면 그때는 SCVP는 원본 요청 안에 있는 인증서가 보낸 (2)에 있는 Application 을 사용하는 인증서에 응답할 것이다.



< 그림 4 > 다른 PKI들의 상호 운영성

그림 4에서, PKI A는 X.509v3 인증서를 발행함으로써 인증한다(PKI A는 위에 보여지는 것과 같이 인증기관(CA: Certificate Authority), OCSP(Online Certificate Status Protocol) 응답기와 LDAP 디렉토리로 구성되어있다). User A는 그때 신호 메시지(1)을 보냄으로써 User B와 교신한다.

User B는 PKI B 아래 인증되고, 그러므로 자연히 신호 메시지의 부분으로 받은 User A의 인증서를 신뢰하지 않을 것이다. 정상적으로 이것은 상호 운영성(Interoperability)이 실패하는 것이다.

그러나 이 경우에, User B는 지역적으로 인증서를 유효화 시키기 위해서 필요하지 않다. 대신에 User B는 SCVP에게 User A의 인증서가 신뢰할 수 있는 것인지를 확인하여야 한다. 그것은 지금 SCVP가 User A의 인증서가 신뢰 될 수 있는 것인가를 결정하는 것에 대해서 책임이 있다. 그것은 PKI A를 확인함으로써 다음 단계로 검증한다.

① User A의 인증서안에 있는 모든 자세한 것들이 여전히 옳은가를 검증한다.

② 그것은 PKI A에 있는 OCSP 응답기를 User A의 인증서가 혹시 폐지되었는지를 검증한다.

모든 검증들은 성공적으로 통과한다는 것을 가정한다. SCVP는 User B에게 User A의 인증서는 유효하다고 한 메시지 (3)을 응답한다. 이 방법에서 2 User들은 PKI A와 PKI B가 같은 계층(hierarchy)의 부분이 되어야 한다거나 그것들을 위해 각각 서로 상대방의 인증 없이 공통이용이 가능하다.

User B는 이 경우에 방어되고 User A는 다른 PKI로부터 왔다는 것조차 알지 못한다. SCVP의 장점으로는 ASN.1과 XML 둘 다 지원을 하고, ASN.1을 위한 Running Code가 벌써 존재한다는 것이다. 반면에 단점으로는 사용자들에게 새로운 이름이라는 것과 여태까지의 프로토콜과는 다른 프로토콜이라는 것이다.

3. 제안된 WPKI 프로토콜의 설계 및 구현

3.1 제안된 시스템의 구성

기존의 PKI 인증 구조는 OCSP방식을 사용하고 있다. OCSP는 인증서의 유효성을 확인하여 상태를 검증하는 방식을 주력으로 하고 있다. 하지만 계속적인 PKI 인증 방식의 변화로 인증서의 상태만이 아닌 변화되는 정책과 인증기관도 파악이 가능한 구조를 요하게 되었다. 이에 현재 여러 가지 방식이 제안되고 있는데 국외에서 SCVP를 가장 선호하는 방식으로 선택하였다.

SCVP는 인증서의 상태검증과 인증경로를 확인하여 발행기관에 대한 정보도 검증하며, 바뀌는 정책에 대한 검증부분이 포함되어있다. 그와 더불어 M-Commerce 환경에서 현재 사용되고 있는 낮은 CPU와 작은 메모리에도 적합한 환경구축을 위한 방법을 제시하고 있다. 클라이언트 장비의 부하를 적게 하기 위하여 대행 서버를 두어 기존에 사용되는 암호화에 따른 장비 부하를 최소한으로 하는 방식을 적용하였다. 하지만 클

라이언트에서 대행 서버로 개인 정보를 넘기는 방식으로 SSL(Secure Socket Layer) 방식을 사용하는데, 이는 Netscape나 인터넷 Explorer에 포함되어 있는 기능으로 실제로 Mobile이나 PDA같은 장비에서 사용하기 위해서는 브라우저의 도움을 받아야 한다는 문제가 생겨, 본 연구에서는 어떤 OS에서도 적용이 가능하여 Platform 독립적이며, 이동 환경에 도움이 될 인증 방식을 제안하려 한다.

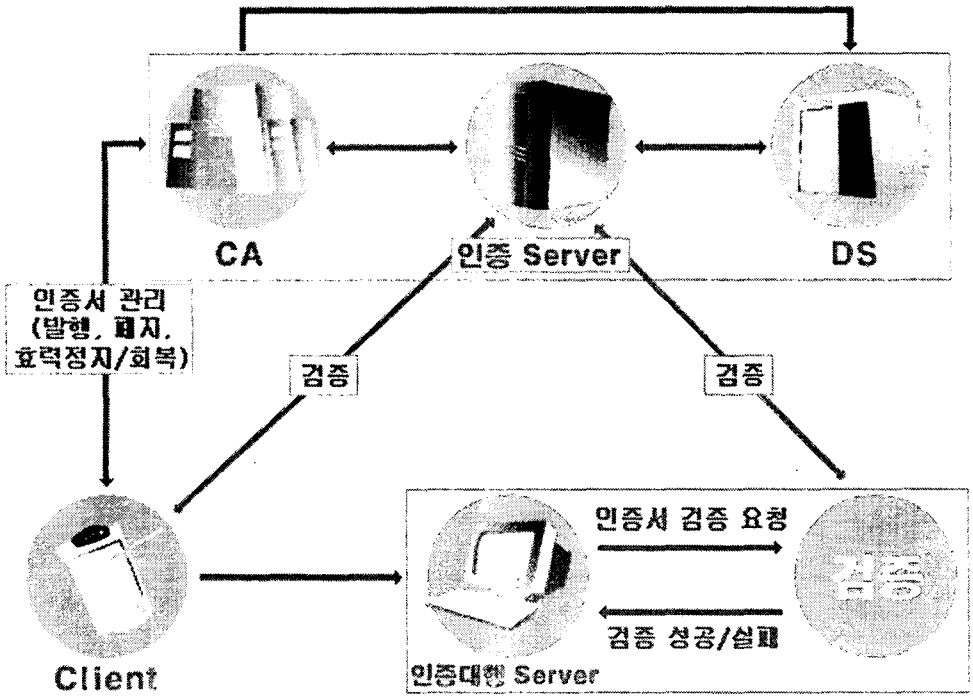
PKI(Public Key Infrastructure)기반의 공개키 암호 시스템을 사용함에 있어서 클라이언트는 상대방의 인증서를 검증해야 한다. 이런 검증단계는 사용자가 신뢰할 수 있는 인증기관이 서명한 것인지 인증서에 포함된 인증기관의 서명이 올바른지 검사하고, 인증서의 사용 용도가 현재 작업에 적합한지와 인증서의 유효기간 등을 검사해야 한다. 그리고 사용자가 비밀키를 저장하고 있던 컴퓨터의 Hard Disk가 Format되거나 Smartcard/USB키를 분실한 경우 등과 같이 인증서의 유효기간이 만료되기 전에 폐지하여야만 하는 경우가 발생할 수 있다. 이로 인해 인증기관 들은 유효기간이 만료되기 이전에 폐지된 인증서의 목록(CRL: Certificate Revocation List)을 유지하여야 하고, 이를 주기적으로 갱신하여야 한다. 인증서 검증단계에서 모든 것이 성공하였다 하더라도 해당 인증서가 CRL에 등록 됐는지를 검사하여야 한다. 이런 작업을 하기 위해서는 클라이언트에 인증서를 검증할 정보가 필요하다. 유선에선 클라이언트가 디렉토리 서버로부터 CRL을 주기적으로 Download하여 사용한다. 그러나 무선환경에서는 제한된 컴퓨터 Power와 메모리를 가지고 있어서 인증서가 사용가능한지를 판단하는 작업의 어려움이 있으며, 주기적으로 CRL를 Download하기 위해 소요되는 시간과 비용으로 인해 적용이 쉽지 않다. 이러한 문제로 인하여 실시간으로 인증서 상태를 검증하고 인증경로를 획득하며 인증된 경로 검증을 위한 프로토콜을 M-Commerce상에서 SCVP를 무선환경에 적용한 시스템 구조는 그림 5와 같다.

3.2 제안된 프로토콜의 설계

WPKI상에서 인증서 상태 검증, 인증 경로 획득, 인증 경로 검증을 위하여 다음과 같이 정의한다.

1. 공개키를 이용하여 정보보호 서비스를 제공하기 전에 먼저 인증서 검증 Routine을 이용하여 수신된 인증서의 유효성을 검증해야 한다.
2. 인증서는 주체의 공개키 정보와 이름을 모아 제3의 신뢰기관(인증기관)의 개인키로 서명함으로써, 공개키 정보의 무결성을 보장해주는 역할을 수행한다.
3. 인증서를 사용하는 신뢰 당사자(인증서를 사용하거나 서명 문을 검증하는 인증서 수신자)는 서명 및 암호 서비스를 위하여 사용되는 공개키를 담고 있는 인증서에 대한 유효성을 먼저 확인한 후 서명 문을 검증하거나 암호문을 생성해야 한다.
4. 인증 경로는 공개키 기반구조 내의 모든 신뢰 당사자가 믿는 "가장 신뢰 된 인증기관"의 서명 된 인증서로부터 시작하여, 하부 또는 네트워크 방식의 공

개키 기반 구조 Model에서 믿음을 서로 확장해주는 하나 이상의 인증기관 인증서들, 그리고 최종 개체 인증서로 구성된다.



< 그림 5 > 시스템 구조도

5. 인증 경로를 검증하는데 이용되는 주요 인증서 확장자는 인증서에 대한 적용 가능한 응용 분야를 나타내고 있는 인증서 정책 Field, 특정의 인증서 정책과 다른 인증서 정책간의 호환 가능성을 나타내는 인증 Mapping Field, 주체 이름이 특정의 이름 공간 내에 존재 하도록 하는 허용 가능한 Sub Tree, 또는 주체 이름이 있어서는 안될 이름 공간을 나타내는 배제된 Sub Tree 등으로 구성된다.

인증 경로 유효성 검증은 클라이언트나 서버의 응용에 존재하거나 별도의 검증 서버에 존재하는 인증 경로 검증 논리에 의하여 수행된다.

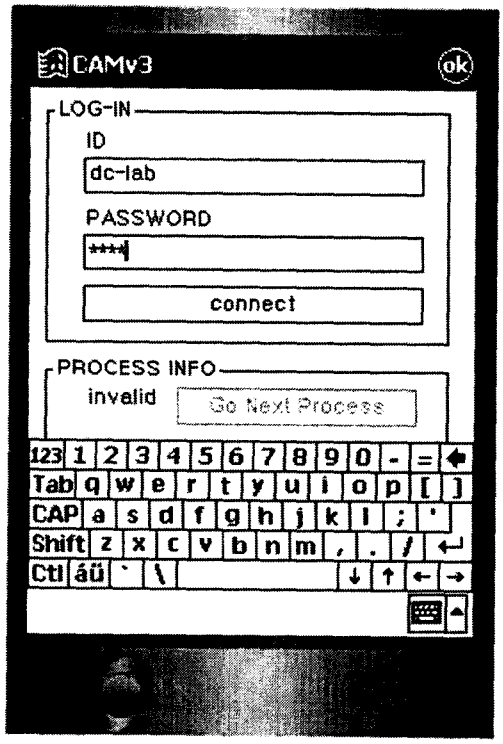
인증 경로의 검증 과정은 검증에 필요한 입력 정보들(인증 경로, 초기 정책 확인자, 그리고 경로 검증이 수행되어야 할 시간 등)을 생성하는 과정, 인증 경로 상의 각각의 인증서에 대해 수행되는 인증서 유효성 검증 과정, 그리고 인증 경로에 대한 인증서 유효성과 검증 과정의 결과를 출력하는 출력부로 구성된다.

인증서 수신자는 거래 상대로부터 인증 경로를 제공받거나 받지 않을 수 있다. 따라서 모든 응용은 인증 경로제공 여부에 무관하게 "가장 신뢰 되는 기관"으로부터 최종 개체까지의 인증서들로 구성된 인증 경로를 먼저 구성해야 하고, 초기에 미리 설정되

어 있는 응용과 관련된 정책 확인자를 이용하여 여기서 획득한 인증 경로의 유효성을 판단해야 한다.

3.3 전자인증서 실험결과

클라이언트는 그림 6에서와 같이 PDA 상에서 SCVP 서버의 인증을 확인 받기 위해 인증 대행 서버에 접속을 시도한다. 접속을 위해서 사용자의 ID와 PASSWORD를 입력하며 connect , Button으로 사전에 정의된 인증 대행 서버에 접속을 시도한다.



< 그림 6 > 클라이언트 PDA에서의 인증 요청

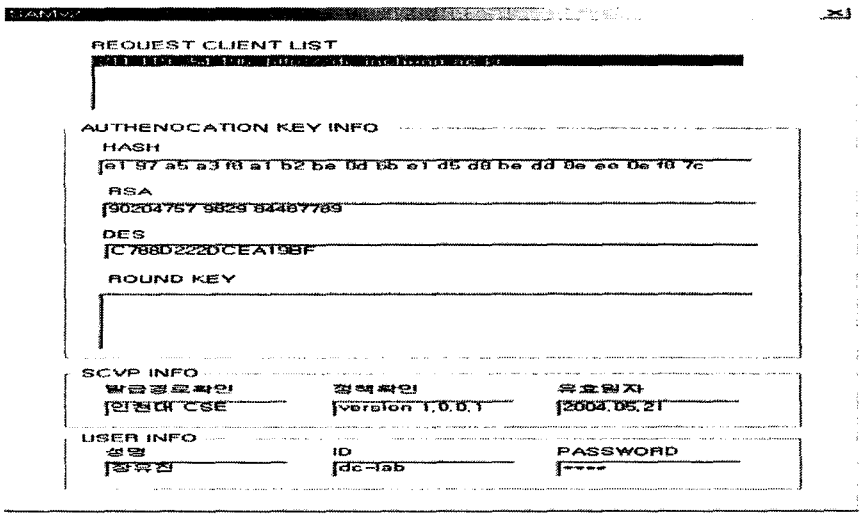
그림 7에서와 같이 인증 대행 서버는 대행 의뢰를 신청하는 요청자의 ID와 PASSWORD를 바탕으로 자신의 DB 상에서 사용자정보를 확인한다. 만일 사용자가 자신의 서버에 등록이 되어 있다면 해당 사용자를 대신해 인증을 요청하기 위해 비밀키와 암호키등을사용해 사용자의 SCVP 정보를 암호화한 후 SCVP 서버에 내용을 전송한다.

그림 8과 같이 인증 SCVP 서버는 자신에게 인증을 요청하는 대행 서버의 Hash 값을 사용해 암호화된 SCVP 메시지를 복호화한다. 암호키를 자신의 DB에서 검색하여 메시지를 복호화한 후 사용자의 SCVP 정보를 확인한 후 그 적법함을 최종적으로 사용자에게 전달한다.

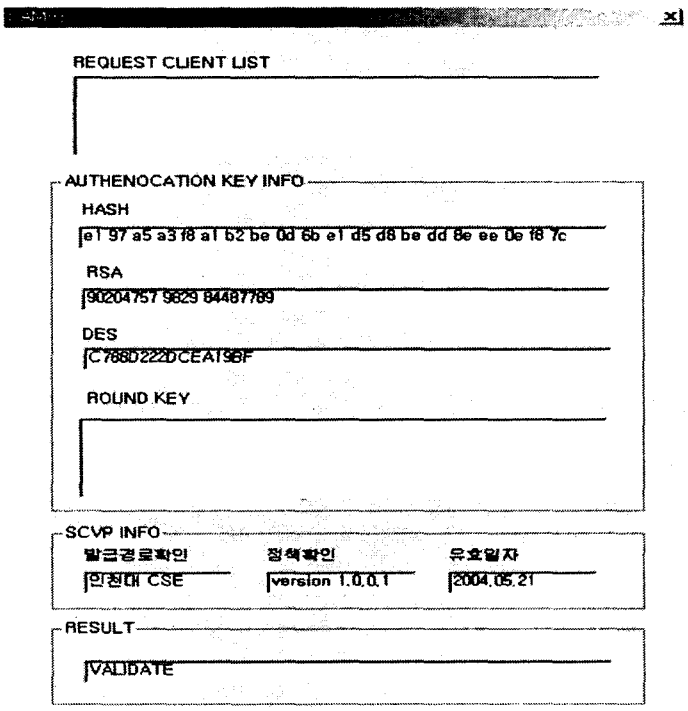
그림 9와 같이 사용자는 최종적으로 자신의 인증의 적합성을 해당 인증 SCVP 서버로부터 확인 받았음을 화면 하단의 PROCESS INFO 창의 하단 상태창의 변화로 감지할 수 있다. 이로서 사용자는 인증권한을 바탕으로 다음 단계로 넘어가서 개인 작업을 지속할 수 있다.

3.4 실험 결과 및 분석

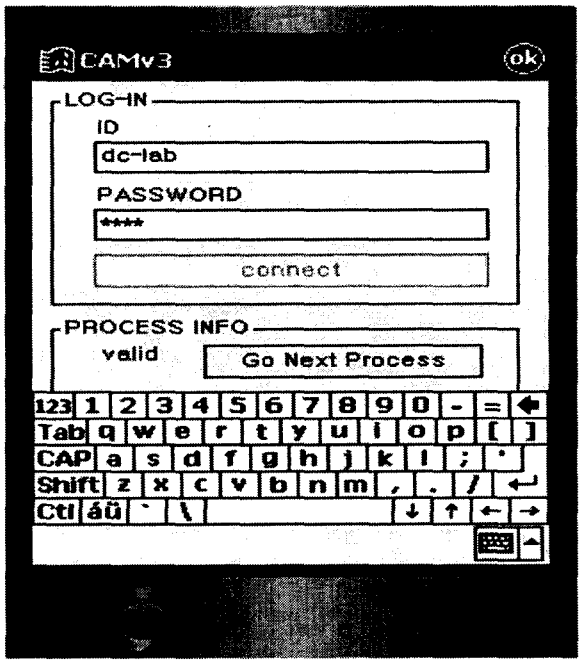
본 연구에서는 SCVP에서 인증서 상태, 발급자 경로 확인, 정책 검증을 통한 시스템을 구현하였고 검증을 위한 전송 방식의 안전한 전송을 위하여 PKI 방식을 사용하여 보안을 제공하였다. 기존의 인증서 사용을 위하여 Active X를 사용하는데 이는 MS사에서 출시된 운영체제에서만 사용이 가능하고 이동 장비나 소형 장비에서는 인터넷 Explorer의 설치가 되지 않기 때문에 사용이 불가능하고 새로운 암호화 모듈을 만들어야 하는 문제가 있다. 이에 현재 IETF에서 제안된 SCVP를 이용하고 PKI방식에서 제공하는 인증 방식을 사용하였다. 이는 새로운 모듈의 추가 없이 어떤 Platform 상에서도 사용이 가능하기 때문에 M-Commerce상에서 효율적으로 사용 가능하다. 그리고 SCVP에서는 클라이언트로부터 검증 요청 메시지를 받아들여야하므로 DoS 공격(Denial of Service Attack)을 받을 수 있는 취약점이 있다. 이에 Signed 메시지를 사용하여 전달 메시지를 관리함으로써 악의적인 공격을 차단할 수 있다. 또한 PKI 방식에서 사용하는 인증 방식을 사용하여 안전한 클라이언트 검증을 할 수 있다. 표1에서 OCSP 와 제안된 시스템을 비교한 결과 인증서 상태정보 표기 와 validation policie의 기능에서 우수한 특성이 나타냄을 얻을 수 있었다.



< 그림 7 > 인증 대행 서버 창



< 그림 8 > 인증 SCVP 서버 창



< 그림 9 > 클라이언트 PDA에서 인증 확인

< 표 1 > OCSP와 제안된 프로토콜의 비교

Protocol	OCSP	제안된 System
Request	양호	양호
Validation Policie	없음	양호
Client에서의 Request 위.변조 검증 방안	양호	양호
인증서 상태정보 표기	미흡	양호
Security Consideration	양호	양호

4. 결 론

전자 상거래의 안전성 보장을 위해 가장 필요한 것은 전자상거래 시에 교환되는 전자 문서에 대한 정보 보호이다. 전자상거래의 거래 규모는 해마다 지속적인 성장을 이루어 왔으며, 현재 도입 단계에 있는 이동 통신 단말기를 이용한 새로운 이동환경의 등장으로 인해, 향후 5년에서 10년 사이에 또 한번 놀랄만한 전자 상거래의 변화와 성장을 이룰 것으로 예상 되고 있다. 하지만 그러한 성장의 이면에는 신용카드의 도용 및 사용부정, 해킹에 의한 신용정보 누출 등의 위험이 끊임없이 도사리고 있다.

따라서 본 연구에서는 2003년 미국의 California주의 San Francisco에서 56번째 인터넷 국제 표준화 기구(IETF: Internet Engineering Task Force)에서, DPD/DPV 표준 프로토콜로 채택한 SCVP를 Model로 하여 인증서 상태, 발급자 경로 확인, 정책 검증을 통한 시스템을 구현하였고 검증을 위한 전송 방식의 안전한 전송을 위하여 PKI 방식을 사용하여 보안을 제공하는 시스템을 설계 구현 하였다. 구현 결과 제안된 시스템은 클라이언트의 책임과 위험부담을 서버측에 위임함으로써 간단히 물건 등을 구매하고, 인터넷 이용을 할 수 있으며, 기존의 OCSP보다 낳은 특성을 얻을 수 있었다. DPD/DPV 프로토콜은 특히 무선기기에 보다 효율적인 방법이다. 왜냐하면 대체로 무선기기는 휴대용으로 되어 있어서, 기기가 작을 수밖에 없다. 그러므로 유선보다는 작은 메모리와 한정된 기능을 가진다. 그래서 무선기기에서의 일을 검증 서버로 위임함으로써 무선기기가 검증을 위해서 더 많은 부품이 필요하지 않다. 이에 SCVP 프로토콜을 사용하여 새로운 모듈의 추가 없이 어떤 Platform 상에서도 사용이 가능하기 때문에 PDA 상에서 효율적으로 사용 가능하고 Signed 메시지를 사용하여 전달 메시지를 관리함으로써 악의적인 DoS 공격(Denial of Service Attack)을 차단할 수 있다. 또한 PKI 방식에서 사용하는 인증 방식을 사용하여 안전한 클라이언트 검증을 할 수 있다.

5. 참 고 문 헌

[1] 염흥열, "DPV/DPD 기능을 갖는 OCSPv2 표준"(2001.8),
http://www.kisa.or.kr/K_trend
/KisaNews/200108/standardization_07.html
[2] 염흥열, "공개키 기반구조 표준화 동향"(2003.3),
http://webzine.kt.co.kr/s-trends/200303/0104.asp
[3] 이석래, "전자서명 인증기술"(2001.3),
http://www.rootca.or.kr/down/down4/Digital%20Signature%20Certification%20Technology.pdf
[4] Santosh Chokhani. Carl Wallace "Trusted Archiving"(2004.4.13),
http://middleware.internet2.edu/pki04/proceedings/trusted_archiving.pdf
[5] A. Malpani. R. Housley. and T. Freeman. "Simple Certificate Validation Protocol" April 2004 http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-14.txt
[6] D. Pinkas. R. Housley "Request for Comments: 3379" (2002.9),
http://www.ietf.org/rfc/rfc3379.txt
[7] T. Polk. And S. Kent. "DPD/DPV Selection" March 2003
http://www.ietf.org/proceedings/03mar/slides/pkix-4/sld2.htm
[8] http://www.ascertia.com/products/tf_scvp/
[9] 이동석 "인증서 검증기술 OCSP/SCVP 표준화 동향"(2001.12.4),
http://www.istf.or.kr/pdf/311_p3.pdf
[10] 박세현, "서버기반 인증서검증 프로토콜 동향 및 SCVP를 이용한 인증서검증 기술"(2003.2.7), "207_서버기반 인증서 검증기술 동향.pdf",
http://www.rootca.or.kr/down/down4/publication.zip

저 자 소 개

장 유 진 : 현재 인천대학교 컴퓨터공학과 석사과정 중
관심분야는 무선 네트워크 구축 등이다.

박 상 민 : 현재 인천대학교 산업공학과 교수로 재직 중이며,
관심분야는 경제성공학, 설비관리, 신뢰성공학, 원가공학

신 승 호 : 현재 인천대학교 컴퓨터공학과 교수로 재직 중이며,
관심분야는 컴퓨터 그래픽스이다.