특집 13

안전한 전자상거래를 위한 보안토큰 기반의 공인인증 방식에 대한 고찰

목 차

이 병 천
(중부대학교)

1. 서 론

공인인증서는 비대면의 온라인 거래에서 상대방의 신분 확인, 전송하는 메시지의 무결성 보장 및 서명, 행위에 대한 부인방지 서비스를 제공함에 있어서, 누구나 인정할 수 있는 사용자 신분 확인을 위한 수단으로 사용된다. 전자서명의 법적 효력을 인정하는 전자서명법[1]이 1999년 제정된 이후 한국은 공인인증체계[2]의 도입과 확산에 노력하였으며, 그 결과 2008년 말 기준으로 2,403만명의 경제활동인구 중에서 77%인 1,856만명이 공인인증서를 사용하는 것으로 나타나 세계적인 성공사례로 제시되고 있다[3]. 이러한 공인인증의 확산은 온라인 상거래의 신뢰성을 향상시켜 전자상거래가 크게 확산되도록 하는 기본 인프라 역할을 하였다. 2008년 기준 한국의 전자상거래 총 거래액은 629조 9,670억원으로 부문별 거래비중을 보면, 기업간 전자상거래(B2B)가 총거래 88.9%인 560조 1,350억원으로 대부분을 차지하고 있으며, 기업·정부간 전자상거래(B2G)가 8.3%, 기업·소비자간 전자상거래(B2C)가 1.9%, 그리고 소비자간 전자상거래(C2C등)는 0.9%로 나타났다. 사이버쇼핑(B2C등)의 2008년 총거래액은 18조 1,460억원으로 전년의 15조 7,660억원에 비해 15.1% 증가하였다[4]. 특히 기업과 소비자간의 상거래가 큰 규모로 이루어지고 있다는 것은 국민들이 우리의 전자상거래 시스템을 신뢰하고 있으며 일상생활을 영위하는데 전자상거래를 거리낌 없이 사용하고 있다는 것을 말해준다. 이러한 공인인증의 확산과 전자상거래의 발전은 세계적으로 유례가 없는 선도적인 사례라고 말할 수 있다.

그러나 우리의 전자상거래 시스템에 대해서는 많은 국민들이 일상적으로 사용하고 있으면서도 여러 가지 비판이 제기되고 있는 것이 사실이다. 액티브엑스 기술에 의존하는 비표준적인 사용환경으로 인한 호환성의 부족, 여러 가지 보안기술의 중복 사용으로 인한 불편과 비효율성, 키보드 해킹, 피싱 등에 의한 각종 보안사고의 사례, 공인인증서 누출사례로 인한 공인인증체계 운영방식에 대한 비판 등은 국민들의 불안을 가중시키고 있다. 심지어는 공인인증의 무용론을 내세우며 공인인증의 의무사용을 해제해야 한다고 얘기하는 의견들도 있다. 그러나 이러한 비판들

로 인해 많은 보안기술들을 선도적으로 적용하여 다른 나라들에 비해 우수한 전자상거래 환경을 구축하고 운영해 온 성과들이 제대로 평가받지 못하는 측면이 있다. 성과에 비해 많은 비판을 받는 것은 그동안 우리가 취약한 PC 환경에 대한 적절한 대책이 없이 비표준적인 기술들을 부적절한 방향으로 사용해오면서 사용자들의 불만을 키워왔던 때문이라고 생각한다.

본 논문에서는 국내외에서 전자상거래를 위해 사용하는 기술들을 비교하고 제기되는 취약점들을 분석해 본다. 또한 이를 해결하기 위하여 하드웨어적으로 안전한 보안토큰을 이용하는 공인인증체계에 대해 설명하고 이의 확산을 위한 정책적 방안에 대해 고찰하고자 한다.

2. 국내외 전자상거래 방식의 비교

먼저 세계 각국의 공인인증체계의 도입 현황에 대해 살펴보자. 세계 각국에서는 공인인증체계의 도입 가능성을 검토하기 위해 각종 시범프로젝트들을 진행하고 있지만 한국을 제외하고는 전국적인 규모로 공인인증체계를 사용하고 있는 국가는 아직 없다. Verisign[5] 등 국제적인 인증업체들은 웹서버 보안 등을 위해 인증서를 발행하고는 있지만 이것은 국가의 공인을 받은 인증체계가 아니다. 더구나 개개인에 대해 인증서를 발행하고 개인이 자신의 신분을 증명하기 위해 인증서를 사용하는 것은 아니다. 그러므로 비대면 온라인 환경에서 상대방의 신분을 인증하기 위한 국제적으로 통용되는 방법은 아직 없다고 볼 수 있다. 실제 전자상거래 환경에서도 ID/pass 등의 전통적인 인증방식을 SSL[6] 등의 통신망 보호기술과 함께 사용하는 수준에 머물러 있다.

외국의 은행들은 ID/pass에 기반한 계정인증을 통해 계좌조회 서비스 등 제한된 서비스만을 제공하며 한국과 같은 실시간 고액 온라인 송금을 허용하지는 않는다고 한다. PayPal[7]과 같은 서비스는 ID/pass에 기반한 계정인증을 통해 PayPal 계정간 실시간 송금을 허용하고 신용카드 계정과 PayPal 계정간 자금이체를 할 수 있도록 하여 전자상거래를 중개하는 서비스이다. Apple[8]사는 애플스토어를 통해 각종 하드웨어, 소프트웨어를 구매할 수 있도록 하고 앱스토어를 통해 음악, 영화, 모바일앱 등 각종 콘텐츠를 구입할 수 있도록 운영하는데, 사용자는 자신의 신용카드 지불정보를 Apple사에 전적으로 위탁해야만 하는 형태로 운영된다.

ID/pass 인증에 기반하는 이러한 전자상거래 방식은 개인과 기업간의 1대 1 신뢰에 의존하는 방식이다. 개인은 개별 기업에게 신용카드 지불정보를 전적으로 위탁해야 하는데 그 기업을 신뢰하지 않고는 실행하기 어렵다. 이미 높은 수준의 신뢰를 구축한 기업이라면 개인들에게 이러한 방식의 상거래를 요구할 수 있겠지만 새로 시작하는 기업들은 소비자들에게 이러한 방식을 요구하기가 어려워 비즈니스 측면에서 큰 진입장벽이 될 수 있다. 개인의 입장에서도 거래하는 기업마다 ID/pass를 설정하여 사용하게 되면 이러한 정보의 관리에 어려움을 느끼게 되는데 거래하는 기업의 수가 늘어날수록 안전한 관리가 더욱 어렵게 된다.

한편 이러한 ID/pass 인증방식은 근본적으로 안전한 인증방식이라고 볼 수 없다는데 더 큰 문제가 있다. 사용자의 기억에 의존해야 하는 패스워드는 단순한 정보의 조합으로 사용하게 되는데 이러한 정보는 어깨넘어 훔쳐보기, 비디오 녹화에 의한 분석 등의 전통적인 방식 뿐만 아니라 온라인 스니핑 공격에도 취약하다. SSL 등의 통신보안 기법을 통해 온라인상의 스니핑을 방지하더라도 사용하는 PC 환경 자체가 해킹에 취약하기 때문에 키로거 등의 여러 가지 방법으로 ID/pass가 외부로 노출될 수 있는 위험이 있다. 또한 여러 사이트에서 동일한 ID/pass를 등록하여 사용하는 것이 일반적인 사용패턴이므로 하

나의 ID/pass가 노출되면 모든 사이트에서 ID/pass가 노출되는 것과 동일하다. 만일 어떤 전자상거래 사고가 발생하여 사용자와 기업간에 분쟁이 발생하면 이것을 해결하는 것이 쉬운 일이 아니다.

반면 국내의 전자상거래 환경은 공인인증체계[2]에 기반하고 있어서 사용자와 기업이 서로의 신분을 확인하는 것이 편리하고 쉽다는 장점이 있다. 사전에 사용자 등록이 되어 있지 않아도 공인인증서에 기반하여 즉시 상대방의 신분을 확인할 수 있고 상거래를 시작할 수 있게 된다. 사용자 입장에서는 여러개의 ID/pass를 기억해야 하는 부담에서 벗어나 공인인증 관련된 정보만 안전하게 관리하면 여러 전자상거래 사이트에서 모두 이용할 수 있기 때문에 편리하며 더욱 안전하게 개인정보를 관리할 수 있게 된다.

한편 전자상거래와 공인인증을 사용하는 PC 환경 자체가 해킹공격에 취약하기 때문에 이를 보완하기 위하여 방화벽, 키보드보안, 피싱방지 등의 PC 보안용 프로그램을 사용하도록 하고 있다. 대표적으로 인터넷뱅킹 시스템에서는 공인인증서를 이용한 인증, 비밀번호의 암호화 저장, 보안카드 또는 일회용비밀번호시스템, PC 보안, SMS 통보 시스템 등 많은 보안도구들을 결합하여 사용하고 있다. 국내의 많은 인터넷 쇼핑몰들은 신용카드결제, 계좌이체, 휴대폰 결제 등 다양한 결제방식을 허용하며 신용카드를 이용한 30만원 이상의 고액결제에서는 공인인증서 사용을 의무화 하고 있다. 인터넷 쇼핑몰에서의 거래시 사용자의 지불정보는 쇼핑몰로 전달되는 것이 아니라 은행, 카드회사, 이동통신회사 등 지불중개기관을 통해 결제되며 사용자는 여러 인터넷 쇼핑몰에서 비슷한 방법으로 거래를 할 수 있기 때문에 거부감 없이 전자상거래에 참여할 수 있게 된다. 거래 결과의 SMS 통보 시스템은 상거래시스템에 대한 신뢰도를 높이고 부정사용을 막는 중요한 역할을 한다.

이러한 사례를 종합해 볼 때 국내의 전자상거래 환경은 공인인증을 통한 사용자 인증과 다양한 보안도구들을 결합하여 사용함으로써 보다 안전한 전자상거래 환경을 제공하고 있다고 말할 수 있다.

3. 국내 전자상거래 방식의 취약점 분석

국내의 공인인증 및 전자상거래 방식은 높은 수준의 보안성을 제공하여 지금까지 성공적으로 운영되고 있지만 그 취약점에 대해 많은 비판이 존재하는 것도 사실이다. 또한 그 취약점은 공인인증 방식 자체의 문제점이 아니라 그것을 사용하는 PC 환경에 근본적인 취약점이 있기 때문이다. 여기에서는 이러한 취약점들에 대한 비판과 그 해결방법에 대해 살펴본다.

3.1 액티브엑스 사용으로 인한 비호환성과 불편

국내의 전자상거래 환경은 공인인증으로부터 쇼핑몰 운영까지 액티브엑스 기술에 기반하여 구축되어 왔다. 액티브엑스 기술은 마이크로소프트의 웹브라우저인 인터넷익스플로러에 연동되어 설치할 수 있는 플러그인 프로그램을 제작하는 기술로 공인인증서를 발급, 사용하기 위한 프로그램을 사용자 PC에 설치하는 손쉬운 방법으로써 초창기부터 국내에서 널리 사용되어 왔다. 국내에서 공인인증과 전자상거래가 확산되면서 윈도우 환경의 운영체제에서 익스플로러를 통해 액티브엑스 기술을 사용한 전자상거래는 당연시 되어 왔다. 그러나 액티브엑스 기술은 여러 가지 위험성으로 인해 표준기술로 인정받지 못하고 있으며 이를 개발한 마이크로소프트마저 사용을 중단하고 있다.

마이크로소프트가 운영체제와 브라우저 환경에서 독점적인 지위를 가지고 있었던 때에는 큰 불만이 제기되지 않았지만 지금처럼 운영체제 환경과 브라우저 환경이 경쟁체제로 바뀐 후에는 비표준 기술을 사용함에 따르는 비호환성이

큰 문제로 대두되게 되었다. 또한 액티브엑스 기술은 전자상거래 구현뿐만 아니라 각종 해킹 프로그램 및 스파이웨어 제작에도 사용되면서 사용자들이 악성 프로그램을 구별하기 어렵다는 측면에서도 큰 위협이 되고 있다.

사용자들이 리눅스, 맥OS, 모바일 운영체제 등 다양한 운영체제와 파이어폭스, 사파리, 크롬, 오페라 등 다양한 브라우저 환경을 사용하게 되면서 국내의 인터넷 환경이 마이크로소프트 환경으로 종속되었다는 비판을 받게 되고 널리 호환될 수 있는 표준적인 기술을 사용할 것을 요구받게 되었다. 최근 국내에서는 표준 기술인 자바를 이용하여 전자상거래 환경을 구축하기 위한 노력이 이루어지고 있다. 국세청 연말정산간소화 서비스, 전자정부의 민원서류 발급 서비스 등은 자바 기반으로 구축되어 여러 가지 운영체제, 브라우저 환경에서 사용될 수 있게 되었다. 지금과 같은 방식의 전자상거래를 가능하도록 하기 위해서는 인증서 관리, 전자서명, 암호화 등을 수행하기 위한 부가적인 소프트웨어를 브라우저에 설치하는 것이 필수적이므로 액티브액스, 자바, 플래쉬 등의 부가적인 기술을 사용할 수밖에 없는데 호환성을 위해 표준기술을 사용해야 한다는 것이다.

3.2 PC 환경 자체의 취약성

현재의 전자상거래 방식에 대한 많은 비판은 공인인증 자체의 취약점 보다는 PC 환경 자체의 취약성에 기인한 바가 크다. 암호화, 전자서명 등 높은 보안성을 가진 암호학적 방법을 쓰더라도 결국은 공개된 운영체제이며 해킹공격에 취약한 PC 환경에서 수행하기 때문에 전자상거래 시스템도 많은 취약점이 존재하게 되는 것이다. 또한 개인이 사용하는 PC 환경은 안전하게 관리되기 어렵고 각종 공격 프로그램에 감염되기도 쉽다. 몇 가지 지적 가능한 취약점 사례들을 보면 다음과 같다.

- 인증서와 전자서명 생성키를 하드디스크, USB 등에 저장하여 사용하는데 공격 프로그램에 감염되면 이들 정보가 외부로 누출될 수 있다.
- 전자서명 생성키를 암호화하여 저장하더라도 키보드 해킹에 의해 사용자 암호가 외부로 누출될 수 있다[9].
- 보안카드를 사용함에 있어서 사용자가 보안카드를 스캔하거나 사진으로 찍어 PC에 저장해 놓고 사용하는 경우 해킹에 의해 외부로 누출될 수 있다.
- PC 환경에서는 공격 프로그램에 감염되면 사용자에게 보여지는 화면과 실제 수행되는 내용이 다르게 될 수 있다.

현재 우리의 전자상거래 환경은 공인인증과 함께 PC 환경의 각종 취약성에 대한 대응책으로 여러 가지 보안기술들을 결합해 사용하지만, 비용 투자를 최소화 하고 사용자 편의성을 높이는 방향으로 설계되어, 결국에는 안전하지 못한 방법으로 사용하고 있는 것으로 생각된다. 예를 들면, 사용자가 공인인증서 관련 정보를 백업하여 다른 PC 환경에서도 설치하여 사용할 수 있도록 허용하고 있는데 해커도 이와 똑같은 일을 할 수 있다. 또한 인증서를 갱신하는 경우 몇가지 사용자 인증 정보를 입력하면 온라인으로 인증서를 갱신할 수 있도록 허용하고 있는데 해커도 정보를 가지고 있다면 똑같은 작업을 할 수 있다. 이에 대한 대책으로 해킹을 방지하기 위한 보안프로그램을 겹겹이 쌓는 것은 근본적인 해결책이라고 볼 수 없다. 현재의 취약한 PC 환경을 피할 수 없다면 사용자의 불편을 감수하더라도 좀 더 안전한 방식을 사용해야 한다. 이러한 PC 환경의 취약성은 컴퓨터를 이용하게 되는 모든 전자상거래 방식에 공통적으로 적용되므로 이에 대한 대응책을 심각하게 고려해야 한다.

이러한 PC 환경에 대한 공격을 방지하기 위해서는 해킹이 어려운 하드웨어 보안토큰(Hard-

ware Security Module)을 사용하는 것이 근본적인 해결책이라고 볼 수 있다. 보안토큰을 사용하면 전자서명이 보안토큰 내에서만 이루어지고 보안토큰 내부에 저장된 중요정보는 외부로 누출되지 않도록 운영할 수 있다.

3.3 보안도구들의 상호 호환성 부족

현재의 전자상거래 환경에서 인터넷뱅킹을 사용하기 위해서는 사용자의 PC에 개인방화벽, 피싱 방지, 키보드보안 등 각종 보안프로그램들을 설치할 것을 요구하고 있는데, 이들 액티브엑스 프로그램들은 여러 은행 사이트들을 사용할 경우 서로 호환되지 않아서 중복 설치되는 경우가 많다. 이미 비슷한 종류의 프로그램을 사용하고 있어도 중복 설치되는 경우가 대부분이며 또한 잦은 업그레이드로 사용자에게 프로그램 설치를 허용할 것을 요구하게 된다. 이러한 불편함은 사용자 PC의 취약한 환경을 은행사이트가 책임지고 보완하도록 의무화했기 때문이며 상호연동에 대한 협의는 부족했기 때문이라고 생각된다. 이로부터 발생하는 문제점들과 사용자의 불편함을 고려하여 기존의 독립된 PC 보안용 프로그램들과 연동되는 형태로 운영하여야 하겠다.

4. 보안토큰 기반의 공인인증 서비스

보안토큰(Hardware Security Module, HSM)이란 전자서명이 저장장치 내부에서 생성되며 저장된 전자서명 생성키는 저장장치 외부로 나오지 않도록 만들어진 하드웨어 장치를 말한다. 이것을 사용하면 피싱, 해킹 등 PC에 대한 공격으로부터 전자서명 생성키를 안전하게 저장할 수 있고 사용자의 전자서명은 보안토큰이 있어야만 생성할 수 있게 된다. PC 환경의 근본적인 취약성을 고려하면 전자서명의 안전성을 보장할 수 있는 근본적인 대응책이라고 말할 수 있겠다.

정부는 보안토큰의 도입을 위해 노력해왔으며 2007년 6월 한국인터넷진흥원 공인인증기관, PKI 전문보안업체, 보안토큰 업체와 공동으로 보안토큰기반의 공인인증서 이용기술 표준화를 완료하고 최상위인증기관을 통해 보안토큰 구현 적합성 평가를 시행하고 있다. 총 19종의 제품이 구현 적합성 평가를 통과하였으며 농협 등 195개 전자상거래 업체에서 보안토큰 기반의 안전한 공인인증서비스를 제공하고 있다[3].

안전한 전자상거래를 위해서는 사용자별 비용이 소요되고 불편함이 있더라도 보안토큰의 도입을 적극 고려해야 한다고 생각하는데 아직 도입에 적극적으로 나서는 곳이 없으며 그 결과로 널리 확산되지 않고 있다.

4.1 보안토큰 기반의 공인인증서 발급 및 사용 방법

보안토큰은 사용자의 공인인증서와 전자서명 생성키를 내장하고 있으며 사용자의 승인에 따라 입력된 메시지에 대해 사용자의 전자서명을 생성하여 출력하는 기능을 가져야 한다. 여기에서는 보안토큰을 이용하는 공인인증체계와 이를 이용하는 전자상거래 방식에 대해 몇 가지 기술적인 측면을 검토해 보고자 한다.

4.1.1 공인인증서 발급

인증기관 또는 등록기관이 사용자 신분을 직접 확인 후 보안토큰에 인증서와 전자서명 생성키를 발급해야 한다. 보안토큰에 저장된 전자서명 생성키는 유일하게 존재하게 되며 외부로 출력하거나 백업할 수 없고 PC에 설치할 수 없다. 보안토큰에 발급되는 공인인증서는 기존의 PC 환경에서 사용하는 공인인증서와 구별되어야 한다.

4.1.2 분실 시 재발급

보안토큰이 분실된 경우 사용자는 인증기관에게 분실을 신고해야 하며 인증기관은 기존의 인증서를 취소하고 사용자에게 새로운 공인인증서 및 전자서명 생성키를 발급해야 한다.

4.1.3 공인인증서 갱신

유효기간이 지나 인증서를 갱신하는 경우 사용자는 인증기관 또는 등록기관에 출석하여 기존의 보안토큰을 제시하고 신분을 확인하여야 한다. 인증기관은 공인인증서를 갱신하여 보안토큰에 저장하고 사용자에게 발급한다. 온라인을 통한 인증서 갱신은 허용하지 않는다.

4.1.4 공인인증서 사용

공인인증서가 내장된 보안토큰은 사용자의 신분을 증명하거나 전자서명을 생성하는데 사용된다. 사용자는 보안토큰을 컴퓨터에 연결 후 필요시 접근암호(PIN)를 입력하여 전자서명을 승인하면 보안토큰은 입력된 메시지에 대해 전자서명을 생성하여 PC로 출력하게 된다. 사용자의 클라이언트 PC는 은행 서버와 보안토큰과의 중개자 역할만 하게 된다.

4.1.5 사용자 전자서명의 저장 및 활용

은행 등 전자상거래 기업은 사용자의 전자서명을 거래의 증거물로서 보관해야 한다. 금융사고 발생시 은행은 사용자의 과실을 입증해야 하는 책임이 있는데 저장된 전자서명은 부인방지 기능을 제공하여 전자서명법에 따라 분쟁을 해결하는 중요한 문서가 된다.

공인인증서를 이와 같이 보안토큰 기반으로 사용하게 되면 전자서명 생성키는 보안토큰 내부에만 존재하게 되어 이것이 없이는 서명을 생성할 수 없게 된다. PC의 환경이 취약하여 해커의 공격을 받고 여러 가지 공격프로그램에 감염되더라도 전자서명 생성키가 누출되는 일은 발생하지 않는다. 이로써 전자상거래 시스템에 대한 공격은 보안토큰에 대한 공격으로 수렴되며 보안토큰이 안전하게 보관되는 한 전체 전자상거래 시스템의 안전성을 보장할 수 있게 된다. 사용자의 전자서명을 부인방지 기능에 사용하게 되면 금융사고에 대한 분쟁해결에 적극 사용할 수 있게 된다.

4.2 보안토큰 발급 정책

현재와 같이 PC 환경에서 공인인증서를 발급, 저장, 서명 생성하는 것은 PC 환경의 근본적인 취약성을 고려할 때 당장 중지해야 한다. 정부에서도 보안토큰 기반으로 공인인증 정책을 바꾸고자 하지만 아직 전이가 원활하지 않은 것은 경제적 비용 문제와 함께 사용자 편의성 문제 때문일 것으로 생각된다. 사용자들은 기존의 무료 공인인증서와 쉽게 백업하고 여러 PC에 설치하여 사용할 수 있는 편리한 공인인증서에 익숙해져 있어서, 보안토큰이 반드시 필요한 유료의 공인인증서를 받아들이기 쉽지 않을 것이다. 또한 액티브엑스와 관련된 현재의 공인인증체계에 대한 불신도 있어서 표준기술을 사용한 편리한 공인인증 서비스체제를 갖추는 것이 급선무이다.

안전한 공인인증체계는 온라인 전자상거래의 확산을 보장하는 핵심 기반구조이며 많은 부가가치를 창조한다. 보안토큰을 이용하는 안전하고 편리한 공인인증체계를 갖추고 약간의 공공비용을 들여서라도 하루빨리 도입하는 것이 좋을 것으로 생각한다. 이와 관련된 몇가지 정책적 측면을 검토해 보고자 한다.

4.2.1 공인인증체계 전환 유도 정책

보안토큰을 이용하는 공인인증서가 안전하고 편리하다고 하더라도 기존에 사용하고 있던 시스템을 일시에 바꾸기는 어려우므로 당분간은 병행 사용 정책을 사용해야 할 것이다. 기존의 PC 기반의 공인인증서는 더 이상 발급을 중단하고 사용 가능한 금액의 상한을 정하는 것이 좋을 것이다. 정해진 금액 이상의 결제를 위해서는 반드시 보안토큰 기반의 공인인증서를 사용하도록 의무화함으로써 점진적인 전이를 유도할 수 있다. 아울러 기존의 PC 기반 공인인증서를 이용하는 경우 취약점이 존재하기 때문에 분쟁이 있

을 수 있고 이 경우 은행이 책임지지 않는다는 점과 보안토큰 기반의 공인인증서를 사용하는 경우 적법한 절차에 따라 은행이 책임진다는 것을 명시하는 것이 도움이 될 것이다.

4.2.2 보안토큰 발급 비용

하드웨어적인 보안토큰을 발급하는 데는 비용이 들게 되는데 기존의 무료 공인인증서에 익숙해 있었던 사용자들의 입장을 고려하여 초기 1회의 발급은 공공비용을 들여서라도 무료 발급하는 것이 좋을 것이다. 분실, 파손 등으로 재발급하는 경우에는 사용자가 비용을 부담하도록 한다. 사용자는 보안토큰의 안전한 보관을 위해 많은 노력을 기울이게 되고 이것은 우리의 전자상거래 시스템을 안전하게 유지하는데 큰 도움이 될 것이다. 공인인증서의 갱신은 기존의 보안토큰에 갱신하게 되므로 무료로 제공할 수 있다.

4.2.3 향후 보안토큰을 이용하는 다양한 응용분야에 대한 고지

보안토큰은 온라인 환경에서 사용자의 신분을 인증하고 서명을 생성하기 위한 핵심 기반구조로서 이를 다양한 온라인 거래에 적용할 수 있다. 예를 들면 온라인 전자투표를 허용한다고 할 때 온라인으로 사용자의 신분을 확인하가 위해서는 전자상거래에 사용하는 보안토큰이 가장 적절한 인증수단이 될 것이다. 이와 같이 다양한 응용분야에 보안토큰 기반의 공인인증서를 사용하게 될 것이라는 점을 사용자들에게 고지하고 지속적으로 추진해 나간다면, 사용자들이 보안토큰 기반의 공인인증의 중요성을 인식하게 되고 성공적으로 전환하는데 큰 도움이 될 것이다.

5. 결 론

본 논문에서는 전자상거래에 사용되는 여러 가지 기술들을 비교 분석하였고, 국내의 공인인증과 전자상거래 방식에 대한 여러 가지 취약점들과 제기되는 비판들을 분석해 보았다. 우리의 공인인증체계에 대한 취약성은 공인인증방식 자체의 취약성이 아니라 사용자가 사용하게 되는 PC 환경의 취약성에 기인한 것이며, 공인인증체계에 대한 비판은 비표준 액티브엑스 기술을 이용하는 것에 대한 불편에 대한 것이다. 이를 해결하기 위해서는 하드웨어 보안토큰을 사용하는 공인인증체계를 사용할 것과 표준기술을 사용한 편리하고 호환성 있는 시스템을 구축해야 할 것이라는 점을 설명하였다. 또한 기존의 PC 환경의 공인인증체계에서 보안토큰 기반의 공인인증체계로 원활하게 전환할 수 있도록 하기 위한 몇 가지 정책적인 측면을 고찰하였다.

안전한 공인인증체계는 온라인에서 사용자의 인증문제를 해결하기 위한 핵심 기반구조로서 온라인 전자상거래의 발전을 보장하는 필수 요소라고 볼 수 있다. 현재의 앞선 공인인증체계를 더욱 발전시켜 전자상거래 선진국으로 자리매김하기 위해서는 안전한 공인인증체계를 갖추는 것이 필수적이라고 생각된다. 약간의 공공비용을 들여서라도 사용자들에게 안전한 공인인증서를 원활히 발급하고 사용자들이 안전하게 사용하도록 유도해야 한다. 아울러 우리의 공인인증체계에 대해 제기되는 여러 가지 비판들에 대해 겸허히 수용하고 토론하여 문제를 해결할 수 있는 시스템을 갖추는 것이 중요하다고 생각된다.

참고문헌

[1] 전자서명법, http://openweb.or.kr/Laws/CertLaw.html

[2] 전자서명인증관리센터, http://rootca.kisa.or.kr/

[3] 국가정보원, 2009 국가정보보호백서

[4] 통계청, 2008년 연간 및 4/4분기 전자상거래 및 사이버쇼핑 동향

[5] Verisign, http://www.verisign.com/
[6] SSL, http://www.openssl.org/
[7] PayPal, https://www.paypal.com/
[8] Apple, http://www.apple.com/
[9] 정태영, 임강빈, "키보드컨트롤러의 하드웨어 취약점에 대한 대응 방안", 정보보호학회 논문지, 제18권, 제4호, 2008. 8.

저자약력

이 병 천

1986년 서울대학교 물리학과(학사)
1988년 서울대학교 물리학과(석사)
2002년 한국과학기술원 정보보호(박사)
1988년~1993년 (주)엘지전선연구소
1993년~1998년 (주)엘지전자기술원
2003년~2004년 호주 Queensland Univ. of Technology 연구교수
2002년~현재 중부대학교 정보보호학과 교수
관심분야 : 암호학, 정보보호, 암호프로토콜, 전자투표, 공인인증체계, 전자상거래 등
이 메 일 : sultan@joongbu.ac.kr