모바일 전자투표 연구동향 및 요구사항 분석

윤 성 현*

목 차

1. 서 론

스마트폰은 단순 전화기능 외에 PC 기반의 이메일, 문서 편집, 전자상거래 등 많은 응용 서비스를 장소에 구애받지 않고 사용할 수 있다. 스마트폰의 다양한 입력 장치와 센서는 GPS 위치추적, 전자지도 서비스, 네비게이션 서비스 등 다양한 응용에 사용될 수 있다 [16].

정보보호 기술은 쇼핑몰, 인터넷 뱅킹, 인터넷 트레이딩과 같이 실생활의 사회적 영역을 전자화하여 사용자에게 많은 편리함을 제공한다. 하지만 전자투표 및 전자현금과 같이 개인 프라이버시와 관련된 사회적 영역의 전자화는 사회적, 기술적, 제도적인 문제로 아직 상용화되지 못하고 있다.

선거는 민주주의 사회에서 정책을 결정하거나 사회의 리더를 선발할 때 국민의 의견을 반영하는 중요한 사회적 행위이다. 국회의선 선거, 대통령 선거와 같은 전국 단위의 선거를 위해서는 선거관리를 위한 위원회 및 조직을 만들어서 후보자, 투표 장소 및 시간을 공지하고 투표지 제작 및 운송을 해야 하는 등 막대한 인력과 비용이 요구된다. 또한, 공정한 선거관리를 위하여 후보자별로 선거관리인단을 구성하고 투표 및 개표 과정을 감시해야 한다.

전자투표는 선거와 관련된 막대한 경비를 절감할 수 있으며 시·공간적 제약을 부분적으로 극복할 수 있으며, 이에 따른 투표 참여율을 높일 수 있다.

인터넷에서 여론조사는 홈페이지를 방문한 사용자들의 투표를 통해서 이루어진다. 이 경우 동일인이 여러 번 투표할 수 있는데 이를 방지하기 위해서는 홈페이지 회원으로 가입된 사용자에 한해서 한 번만 투표할 수 있도록 해야 한다. 더불어 사용자의 투표 행위를 기록하여 중복 투표가 발생할 수 없도록 해야 한다. 선거는 법적인 절차에 의해서 인증 받은 사용자만이 투표에 참여할 수 있고, 누가 누구에게 투표했는지 알 수 없어야 한다. 따라서 중복 투표를 방지하기 위해서 투표 행위를 모두 기록하게 되면 프라이버시 보호 문제를 야기하게 된다.

전자투표는 선거의 모든 단계를 전자적으로 처리하는 방식과 (인터넷 기반 전자투표), 투표 및 개표 단계의 일부만을 전자화하는 방식으로 (부분 전자투표) 구분된다 [1].

인터넷 기반 전자투표는 비대면 공간에서 투표에 참여한 유권자의 신분이 법적으로 유효한지, 유권자 본인임이 틀림없는지를 증명할 수 있어야 한다. 더불어 매표 및 강압에 의한 투표를 할 수 없도록 하는 기술적, 제도적인 해결 방안이 제시되어야 한다.

현재 미국, 인도 등 전자투표를 도입하거나 추진중인 대부분의 국가는 투표 또는 개표 단계의 일부를 전자화하는 부분 전자투표 방식에 초점을 맞추고 있다. 유권자는 기존의 선거 방식과 마찬가지로 직접 투표 장소에 방문하여 선거관리자에게 본인임을 증명하

* 백석대학교 정보통신학부 조교수

고 지정된 장소에서 전자식 투표 기기를 이용하여 투표한다.

이러한 전자투표의 장점은 기표를 위한 투표지가 필요 없어서 경비가 절감되며, 투표지에 기표를 잘못하여 발생하는 무효표 등 투표 오류를 최소화할 수 있다는 것이다. 또한 개표를 전자화함으로써 개표 단계의 오류를 최소화할 수 있고 유권자들에게 신뢰성 있는 개표 결과를 바로 제공할 수 있다 [1].

하지만 유권자들은 전자식 투표 기기를 전적으로 신뢰해야 하며, 기존 선거에서는 후보자의 요청으로 재검표가 가능하지만 전자투표에서는 재검표가 어려운 단점이 있다.

유권자들에게 전자식 투표 기기의 신뢰성을 보장하려면 유권자들의 투표가 개표에 반영되었는지 확인할 수 있도록 증거를 제공해야 한다. 하지만 영수권을 (투표의 증거) 발행하게 되면 유권자가 다른 사람에게 내가 누구에게 투표했는지 증명할 수 있기 때문에 투표권 매표가 가능하게 된다. 결국 영수권은 유권자 본인만 검증의 성공 여부를 판단할 수 있고 다른 사람은 검증 결과를 설명해도 성공한 것인지 또는 실패한 것인지 판단할 수 없는 특성을 가져야 한다 [7].

사회적 영역은 매우 다양하기 때문에 각 영역의 전자화를 위해서는 그 특성에 따라 실용화를 위한 다양한 요구사항과 해결 방안을 제시해야 한다. 투표는 개인 프라이버시 보호와 연관되며 선거 규모 및 종류에 따라서 전자화 요구사항이 변하기 때문에 전자투표 기법을 위한 단일 솔루션을 제시하는 것은 매우 어렵다 [2].

2012년은 지방선거, 국회의원 선거, 대통령 선거 등 대규모 선거가 예정되어 있고 때마침 스마트폰의 대중화로 모바일 투표에 대한 수요가 증가하고 있다. 본 논문에서는 스마트폰을 이용하는 모바일 환경에서 장소에 구애받지 않고 투표할 수 있는 모바일 전자투표 요구사항과 연구 동향을 살펴본다. 모바일 전자투표를 구현하기 위해서는 등록, 투표, 개표로 구성되는 선거의 전 단계를 전자화하는 인터넷 기반 전자투표 방식이 이상적이다.

2 장에서는 인터넷 기반 전자투표와 부분 전자투표 방식에 대해서 살펴본다. 3 장에서는 스마트폰을 이용한 에스토니아의 인터넷 기반 전자투표 방식을 분석한다. 4 장에서는 모바일 투표를 위한 필수 요구사항 및 관련 연구를 분석한다.

2. 전자투표 방식

2 장에서는 부분 전자투표 방식과 인터넷 기반 전자투표 방식에 대해서 살펴본다.

2.1 부분 전자투표 방식

부분 전자투표는 투표 또는 개표 단계의 일부분을 전자화한 것으로 선거와 관련된 제반 경비를 절감하고, 투표 및 개표 오류를 최소화함으로써 선거의 효율성과 신뢰성을 높인다. 유권자 신분 확인은 기존의 선거와 동일하게 지정된 투표 장소에서 이루어지며, 매표 및 강권 투표를 방지하기 위하여 선거관리인단의 감시 하에 전자투표를 하게 된다. 부분 전자투표 방식은 기계식 투표와 전자식 투표로 구분된다.

(1) 종이 투표 방식 (Paper based voting) [1]

현행 투표 절차는 유권자로 하여금 본인이 기표한 투표지를 투표함에 넣으면 본인의 투표가 개표에 반영된다는 확신을 갖도록 한다. 또한 기계식 개표에 의하여 오차 범위 이내로 결과가 나오거나 또는 후보자가 선거 부정 의혹이 있다고 판단될 시 재개표를 요구할 수 있다. 종이 투표 방식은 유권자의 투표지가 투표의 증거가 되므로 재개표가 가능하다. 단점은 투표지 제작, 배송, 관리를 위한 비용이 많이 요구되고, 투표지에 기표 도장을 찍는 과정에 유권자에 의한 실수가 발생하여 무효표로 처리될 확률이 높고, 개표 과정에 사람이 개입하여 수작업으로 후보자별 투표지를 분류하는 과정에서 실수로 다른 후보자를 지지하는 투표지가 섞일 수 있다는 것이다. 이러한 수동적인 투개표 방식에 기인한 오류율이 높아지게 되면 선거 방식에 대한 신뢰성이 저하된다.

(2) 기계 투표 방식 (Mechanical voting) [1]

기계 투표 방식은 투표 및 개표 기능을 갖는 기계를 이용하는 것으로 유권자는 투표 및 개표 기계가 오류 없이 정확하여 자신의 투표가 개표에 반영된다

는 확신을 가져야 한다. 종이 투표 방식과 비교하여 제반 비용이 절감되지만, 유권자의 투표 증거가 남지 않기 때문에 선거에 대한 의혹이 발생할 경우에 재검표가 불가능하고 유권자들 모두가 투표를 다시 해야 하는 단점이 있다. 선거 결과를 재증명할 수 있는 증거가 남지 않는다는 것은 기계식 투표의 신뢰성을 저하시키는 주요 요인이다.

(3) 전자투표 방식 (Electronic voting)

부분 전자투표는 컴퓨터 소프트웨어를 이용하여 투표 및 개표를 하는 것을 의미한다. 미국의 DRE Voting Machine은 유권자의 기표 오류를 최소화하기 위해서 도입된 시스템으로 유권자는 투표 및 개표에 사용된 DRE 소프트웨어를 전적으로 신뢰해야 한다. 미국 대선에 사용된 DRE 소프트웨어는 기계 투표 방식과 마찬가지로 투표의 증거를 남기지 않아서 재검표가 불가능하였다. 이러한 제약은 전자투표 방식에 대한 비평가들의 많은 논란을 불러 일으켰으며 DRE 프로그램이 투표의 증거를 남기도록 수정하는 근거가 되었다. 개별 검증을 위한 방법으로 보이지 않는 잉크로 (Invisible Ink) 투표권을 프린트하고 특수펜으로 이를 볼 수 있도록 하는 방법을 권장하고 있다 [4].

A. S. Tannenbaum은 [5]에서 전자투표 소프트웨어는 소스코드가 공개되어야 하고 유권자는 본인의 투표를 개별적으로 검증할 수 있어야 한다고 제안하였다.

2.2 인터넷 기반 전자투표 방식

인터넷 기반 전자투표는 사용자 등록, 투표, 개표로 구성되는 선거의 모든 단계를 전자화하는 것이다. 국회의원 선거, 대통령 선거와 같이 모든 유권자들이 참여하는 대규모 전자투표를 위한 요구사항은 다음과 같다 [1, 5, 7, 9].

1. 재사용 불가(Unreusability)
   투표권을 복제하여 이중 투표할 수 없다.
2. 익명성(Privacy, Anonymous)
   투표 결과로부터 누가 누구에게 투표했는지 유추할 수 없고 전송된 투표권을 추적할 수 없어야 한다.
3. 위조 불가(Unforgeability)
   제 3자가 법적 효력을 갖는 투표권을 만들 수 없다.
4. 합법성(Legality)
   등록된 유권자만이 전자투표에 참여할 수 있다.
5. 완전성(Completeness)
   개표 결과에 모든 유효표가 반영되어야 하고 전자투표 프로그램은 버그가 없고 해킹할 수 없도록 코딩되어야 한다. 또한 프로그램 소스는 공개되어야 한다.
6. 강건성(Robustness)
   투표 및 개표 과정에서 선거관리자에 의한 공모 및 결탁을 최소화하기 위하여 선거관리 센터의 권한을 분산해야 한다.
7. 개별검증(Self Verification)
   유권자는 본인의 투표가 개표에 올바르게 반영되었는지 확인할 수 있어야 한다.
8. 전체검증(Universal Verification)
   모든 구성원이 전체 개표 결과의 유효성을 확인할 수 있어야 한다.
9. 매표방지(Vote Selling)
   유권자는 다른 사람에게 투표권을 팔 수 없고 본인의 투표권으로 누구에게 투표했는지 증명할 수 없어야 한다.
10. 강권투표(Vote by Coercion)
    투표권 등록 및 투표 단계에서 제 3자가 참여하여 감시할 수 없어야 한다.
11. 투표취소(Vote Cancellation)
    투표 기간 중에 유권자의 의사에 따라서 이전 투표를 취소하고 재투표할 수 있어야 한다.

가상공간에서 사용자의 신분을 확인하는 것과 매표방지 요구사항을 구현하는 것이 현실적으로 쉽지 않기 때문에 실제 사례 보다는 이론적 연구가 대부분이며, 이중 투표 및 개인 프라이버시 보호와 관련된 연구가 주로 진행되었다. 최근에는 투표권 추적이 불가능한 믹스넷과 투표권 개별 검증 방법이 주요 연구 이슈로 부각되고 있다.

믹스넷은 D. Chaum이 제안한 추적할 수 없는 통신 채널 [8] 개념을 구현한 것으로 유권자가 전송한 투표권을 추적할 수 없게 한다. 유권자가 네트워크로 전송한 전자투표권은 IP 패킷에 포장되는데, IP 패킷의 소스 주소를 추적하면 누가 누구에게 투표했는지 알 수 있게 된다.

믹스넷 서버는 유권자들의 전자투표권을 모아서 랜덤하게 섞고 발신지를 추적할 수 없도록 설계한다. 서

버는 투표함의 역할을 암호학적으로 구현한 것으로 복수의 입력 값들을 서버가 복호화 또는 재암호화하여 메시지 내용은 변화시키지 않으면서 순서를 바꾸어 입출력 상호관계를 감춘다.

믹스넷과 더불어 선거의 공정성을 실현하기 위한 요구사항으로 전체 검증, 개별 검증, 매표 방지가 있다 [1, 7].

전체 검증은 선거에 참여한 모든 유권자들의 표가 개표 결과에 올바르게 반영되었는지 검증하는 것이다. 단점은 국회의원 선거, 대통령 선거 등과 같은 대규모 선거에서 전체 검증에 실패하면 선거를 다시 진행해야 하는 부담이 따른다는 것이다.

개별 검증은 유권자 개개인이 자신의 표를 검증하는 것으로 투표 후에 영수권을 받고 이를 이용하여 본인의 표가 올바르게 개수되었는지 확인할 수 있다 [7, 11].

매표 방지는 투표권 매수를 할 수 없도록 하는 것이다. 현행 선거는 정해진 투표 장소에서 유권자의 투표 행위를 선거관리인단이 공동으로 감시함으로써 이를 방지한다. 전자투표에서는 투표의 증거인 영수권으로부터 누가 누구에게 투표했는지 유권자 본인 이외에는 유추할 수 없어야 매표를 방지할 수 있다.

인터넷 기반 전자투표를 실용화한 사례로는 스위스와 에스토니아가 대표적이다. 스위스 전자투표 시스템에서 유권자들은 투표를 위해서 컴퓨터 또는 스마트폰을 이용할 수 있다 [3]. 시스템은 두 단계로 투표권을 암호화 하는데 여기에 사용되는 키는 유권자들의 메일로 전송된 패스워드를 이용한다. 에스토니아의 i-voting 시스템은 PKI 인증서가 저장된 ID 카드를 이용하여 투표하는 방식이다. 기존의 선거에서 사용된 투표 봉투 개념을 디지털 봉투에 (digital envelope) 적용하였다 [2].

3. PKI 기반의 모바일 투표 〔2〕

3 장에서는 지역 선거, 의회 선거에 PKI 기반의 인터넷 전자투표를 도입한 에스토니아의 사례를 살펴본다.

에스토니아의 ID-PKI는 (ID 카드 기반의 PKI) 본인 인증이 필요한 인터넷 뱅킹, 디지털 서명, 전자투표와 같은 서비스를 이용할 수 있게 한다. 인증기관 CA는 (Certificate Authority) 국가로부터 공인 받아야 하며 사용자들의 공개키 인증서를 발급한다. 인증서는 사용자 신분과 사용자 공개키를 연결한 (binding) 것으로 법적 구속력이 있으며 ID 카드에 저장한다.

ID-PKI는 은행 및 전자투표에 응용되는데, 에스토니아 중앙은행은 ID-PKI 보안 규격을 준수하기 위하여 일정액 이상의 모든 거래에 대해서 ID 카드로 인증 및 허가를 받도록 하고 있다. 또한 ID-PKI는 인터넷 기반의 전자 선거에 사용되는데, 2005년의 에스토니아 지방선거, 2007년의 에스토니아 의회선거, 2009년의 범유럽 의회 선거가 그 예이다.

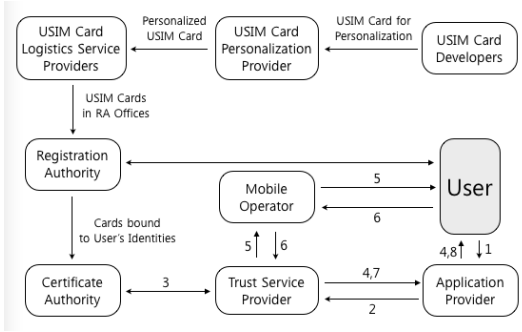
ID-PKI 서비스를 이용하기 위해서는 항상 컴퓨터와 ID 카드 리더기가 있어야 한다. 카드 리더기는 언제 어디서나 필요할 때 항상 사용할 수 있는 것이 아니고 특히 컴퓨팅 환경이 갖추어져 있지 않은 건물 외부에서는 더욱 사용하기 쉽지 않다. PKI 서비스의 가용성을 높이기 위해서 컴퓨터와 카드 리더기 기능을 통합할 수 있는 스마트폰을 이용하는 것이 이상적이다. 인증 및 디지털 서명을 하기 위해서 컴퓨터 또는 USIM이 내장된 스마트폰을 이용한다. 스마트폰을 이용한 인증과 서명은 소프트웨어 기반 서비스 SaaS, 클라우드 컴퓨팅 환경에서 필수적이다.

에스토니아의 Mobiil-ID 표준은 스마트폰을 이용한 개인 식별 및 인증을 위해서 사용된다. Mobiil-ID USIM은 일반적인 SIM 카드 기능과 더불어 인증 및 서명을 위한 개인키를 통합한다. 따라서 ID 카드의 개인키를 불러오기 위한 카드 리더기가 없어도 된다. Mobiil-ID는 WPKI(Wireless Public Key Infrastructure)에서 사용자 신분 인증을 위한 용도로 사용된다 [19].

3.1 WPKI 인증

WPKI는 사용자 인증과 부인봉쇄 서비스를 제공한다. (그림 1)은 에스토니아의 WPKI 인증 프로토콜로 전자투표 및 모바일 결재 시스템을 지원한다 [20].

USIM 카드 제작자는 (USIM card developers) USIM 카드를 개인화 할 수 있도록 만든다. USIM 카드 개인화 제공업체는 (USIM card personalization provider) 인증과 서명에 필요한 사용자 개인키와 공개키 쌍, 2 개의 PIN (Personal Identification Number)과 PUK를 카드



(그림 1) WPKI 인증 단계

에 저장한다. USIM 카드 물류 서비스 업체는 (USIM card logistics service providers) 개인화된 USIM 카드를 RA로 (Registration Authority) 배송한다.

RA는 CA를 대신하여 사용자 등록과 USIM 카드 발급, 사용자 민원 처리를 한다. CA는 인증서 발급, 일시정지, 취소, 보관 업무를 관리한다. TSP는 (Trust Service Provider) MO (Mobile Operator), CA와 통신하여 AP의 (Application Provider) 인증 및 서명 요청을 처리한다. MO는 사용자와 TSP 간의 통신을 중개하기 위하여 OTA (Over The Air) 서버 또는 SMS 센터를 이용한다.

(그림 1)의 WPKI 인증 단계에서 사용자는 컴퓨터와 USIM 카드 U가 삽입된 스마트폰이 있다고 가정한다. USIM 카드 U는 사용자 공개키-개인키 쌍 (k, k^{-1})와 개인키 인증 및 접근에 필요한 PIN 코드를 내장하고 있다. 서버 S가 제공하는 서비스를 이용하기 위해서는 다음과 같은 WPKI 인증 프로토콜이 수행되어야 한다.

단계 1:	사용자는 서비스에 접근하여 I를 포함하여 S에게 인증 요청을 보낸다.
단계 2:	S는 TSP에게 I를 식별해줄 것을 요청한다.
단계 3:	TSP는 CA와 함께 I의 인증서를 검증한다.
단계 4:	TSP는 검증코드 V를 S에게 보낸다.
단계 5:	S는 V를 사용자 컴퓨터로 전달한다. S는 코드 V를 포함한 인증 요청이 스마트폰으로 갈 것이고 이 두 값이 일치하는지 사용자가 검증해야 한다는 것을 알려준다.
단계 6:	TSP는 V를 해쉬코드 H와 함께 MO를 경유하여 사용자 스마트폰으로 전송한다. V 코드를 점검할 것을 요청하고 인증 PIN을 사용자에게 지급한다.
단계 7:	사용자는 PIN을 스마트폰에 입력하고 인증된 개인키 k^{-1}로 H를 서명한다.
단계 8:	TSP는 사용자 서명을 검증하고 그 결과를 AP로 전송한다.
단계 9:	AP는 TSP로부터 수신한 서명 검증 결과에 따라서 사용자를 인증하거나 인증 단계를 취소한다.

3.2 WPKI 위험 분석

MO의 서브시스템인 OTA 서버와 SMS 센터간의 통신은 MITM (Man In The Middle) 공격을 야기한다. (그림 1)의 인증 단계에서, MO는 사용자 ID I, 검증코드 V, 해쉬코드 H 그리고 H에 대한 서명을 중개한다. 해커는 MO와 마찬가지로 사용자와 서버 간에 주고받는 메시지에 접근할 수 있다. 해커는 식별자 I를 수정하여 MITM 공격을 시도할 수 있다.

MITM 공격을 포함한 여러 공격에 대응하기 위해서는 SSL/TLS 또는 동일한 보안 수준을 갖는 인증 기법을 MO 서브시스템이 기본으로 제공해야 한다. 서브시스템 채널을 보호하는 것은 WPKI 사용자 등록과 인증서 처리를 위해서 매우 중요하다.

MITM 공격 외에 또 다른 위험요소는 해커와 사용자가 짧은 시간 간격을 (수 초 이내) 두고 동일한 아이디로 동시에 접속할 경우 해커에 의한 가장 공격이 가능하다는 것이다. 해커는 컴퓨터를, 사용자는 스마트폰을 이용할 경우에, 스마트폰 인증을 위한 PIN 코드 입력 도중에 해커의 컴퓨터로 인증 값이 먼저 도착하게 된다. 이러한 공격에 대응하기 위해서, 동일한 사용자로부터의 인증 요청이 동시에 여러 곳에서 오게 되면 AP가 그 요청을 거부하도록 프로그램 되어야 한다.

(1) MITM 공격

해커는 SSL/TLS 기능을 갖는 서버 S와 클라이언트 C 사이에서 다음과 같이 공격한다.

단계 1:	사용자는 S가 제공하는 웹사이트가 아닌 해커 A의 웹사이트로 디렉션된다.
단계 2:	C는 응용 계층에서 상호 인증된다.

단계 3:	A는 C의 요청에 응답한다. 그리고 응용 계층에서 C와 A, A와 S를 연결하는 두 개의 세션을 생성한다.
단계 4:	A는 두 세션에 쉽게 접근할 수 있다. 인증 데이터를 중개하고 C와 S 사이의 향후 트랜잭션을 기다린다.

일회용 패스워드 같은 인증 기법과 비교하면 WPKI 기반의 인증 기법은 보다 다양한 공격에 대처할 수 있다. 예를 들면, 해커 A는 S와 단독으로 통신할 수 없고 항상 사용자가 연결되어 있어서 PIN 코드를 제공해야만 A와 S의 연결이 가능하다. 그럼에도 불구하고, A는 C와 S간의 WPKI 인증 단계에서 언제든지 중간에 개입할 수 있어서 MITM 공격이 가능하다.

반면에, ID-PKI는 SSL/TLS 핸드쉐이크 중에 사용자 인증서와 서버 공개키 인증서를 가지고 사용자와 서버를 인증하는 단계가 포함된다. 따라서 A는 C의 SSL/TLS 세션키에 접근할 수 없으며 MITM 공격이 사실상 불가능하다.

WPKI에서의 MITM 공격에 대한 대응 방안으로 사용자가 주요 트랜잭션을 디지털 서명하도록 함으로써 실시간 MITM 공격을 기술적으로 매우 복잡하게 만들 수 있다. 이 경우 A는 S의 역할을 사용자에게 그대로 재현해야 한다.

토큰을 이용한 TLS-SA 인증 기법은 WPKI 보안을 한층 강화할 수 있다 [22]. TLS-SA에서 사용자 인증은 SSL/TLS 세션과 관련된 상태정보, 사용자 신임정보가 있어야만 가능하다. TLS-SA 인증 세션은 다음과 같은 단계로 진행된다.

단계 1:	C의 초기 TLS/SSL 세션 정보를 해쉬하여 해쉬코드를 만들고 사용자 컴퓨터의 웹브라우저를 이용하여 스마트폰으로 전송한다.
단계 2:	사용자는 스마트폰 화면에 표시된 해쉬코드를 스마트폰에 입력하고 MO와 TSP를 거쳐서 서버로 전송한다.
단계 3:	서버는 SSL/TLS 세션이 사용자가 시도한 세션과 동일한 지 점검함으로써 MITM 공격을 무력화할 수 있다.

TLS-SA를 구현하려면 WPKI 프레임워크를 수정해야 한다. 더불어 몇 몇 WPKI 메시지를 수정해야 하고 사용자가 직접 해쉬 코드를 입력해야 한다. 사용자에 의한 직접 입력을 피하기 위해서는, 스마트폰이 컴퓨터와 연결되어 서로 메시지를 주고받을 수 있으면 된다. 예를 들면, 블루투스 기술을 이용하여 스마트폰과 컴퓨터를 연결하거나 스마트폰으로부터 서버와 TSP로의 통신이 가능하면 된다. 스마트폰과 WPKI 구성 요소간의 통신 기능이 추가되면 이에 대한 보안 분석도 추가로 요구된다.

3.3 모바일 투표 (M-Voting)

전자투표는 선거와 관련된 다음과 같은 별도의 요구사항을 만족해야 한다.

1. 전자투표권은 반드시 익명으로 남아야 한다는 것과 전자투표 시스템은 모든 기록을 남겨야 한다는 서로 상충되는 요구사항을 동시에 만족해야 한다.
2. 투표 결과는 오류가 없어야 하며 모든 구성원이 납득할 수 있어야 한다.

에스토니아 i-voting 시스템은 전형적인 오프라인 선거에서 사용된 투표 봉투 개념을 디지털 봉투 (digital envelope)에 적용하였고 다음과 같은 단계로 구성된다 [6].

단계 1:	암호화된 투표권은 봉투 안에 디지털 서명은 밖에 있도록 디지털 봉투를 만든다.
단계 2:	유권자들은 공개키 인증서로 본인임을 입증한다.
단계 3:	투표 시스템의 공개키로 자신의 투표권을 암호화 한다.
단계 4:	자신의 개인키로 암호화된 투표권을 서명한다.
단계 5:	투표 시스템은 투표권을 수집하고, 정렬하고, 검증한다.
단계 6:	디지털 서명은 암호화된 투표권과 분리되고 유권자 리스트를 만드는데 사용된다.
단계 7:	투표 시스템은 자신의 개인키로 투표권을 복원하고 그 결과를 개수 한다.

모바일 투표 관리 조직은 WPKI 요구사항을 설정하고 평가해야 한다. CA의 기능을 갖는 전자 정부 또는 관련 부처는 USIM 카드 개발자, 카드 커스터마이징 제공자, 카드 배송 사업자들을 선택하는 기준을 평가해야 한다.

RA 또는 MO는 WPKI 인증서가 포함된 USIM을 등록하기 위하여 사용자에 대한 신분 확인을 엄격한 절차로 관리하고 문서화하고 정기적으로 감시해야 한다. 이 절차는 ID 카드를 발급하는 절차와 비교할 수 있어야 한다. 사용자 신분 확인이 MO에서 가장 중요한 일은 아니지만 이런 과정이 없으면 기존의 SIM 또는 USIM 카드는 법적인 신분을 표현하는 수단으로 활용되기 어렵다.

모바일 투표 조직 및 CA는 적극적으로 사회적 위험요인을 줄여야 한다. 모바일 투표에 대한 보안 위험성을 다음과 같이 사람들에게 알려야 한다.

1. 사용자들은 서명 서비스가 가능한 스마트폰을 다른 사람에게 빌려주어서는 안 된다.
2. 인터넷 카페와 같은 공공 장소에서 스마트폰을 이용하여 디지털 서명을 해서는 안 된다.
3. 스마트폰에 대한 위협요소, 스마트폰 보안 수칙 위반, 바이러스, 등등을 고려해야 한다.
4. CA는 사용자들로 하여금 ID 카드, USIM 카드와 연관된 모든 인증서들을 그들의 상태와 과거 정보를 포함하여 검토하도록 한다.

ID 카드는 정부에서 공식적으로 발급한 카드이다. 따라서 ID 카드 소유자는 법적 구속력을 갖는다. 예를 들면, ID 카드를 소지하고 있는 사용자가 자신의 ID 카드에 있는 정보를 변경하면 이를 정부에 공지해야 한다. 모바일 투표에 접목하기 위해서, (법적 구속력을 확보하기 위해서) WPKI를 위해 사용되는 USIM 카드가 ID 카드와 동일한 효력을 가져야 한다.

유권자들이 모바일 투표를 사용하기 위해서는 MO에서 WPKI 서비스를 제공해야 한다. 모바일 투표를 위한 WPKI는 2048 비트 RSA 키와 SHA-2 해쉬함수를 이용한 인증서를 제공할 수 있어야 한다. 또한 스마트폰용 전자투표 소프트웨어 개발자들은 CC 프레임워크를 준수해야 한다. (Common Criteria Framework)

4. 모바일 투표 요구사항

4 장에서는 모바일 투표 실용화를 위한 요구사항, 관련 연구 그리고 해결 방안을 분석한다.

4.1 모바일 투표 요구사항

모바일 투표를 선거에 적용하기 위해서는 다음과 같은 사안을 고려해야 한다.

○ 네트워크를 이용한 비대면 사용자 인증

선거의 가장 기본적이고 중요한 요구사항 중의 하나가 바로 유권자 본인이 투표에 참여해야 한다는 것이다. 민주주의 선거에서 나의 투표 권리를 다른 사람에게 양도해서는 안 된다. 기존 선거는 투표 장소에서 선거관리자가 유권자의 신분을 대면하여 확인함으로써 이 요구사항을 만족한다.

스마트폰을 이용한 모바일 투표는 인터넷을 이용하여 비대면으로 신분 인증을 해야 된다. 3 장의 에스토니아 모바일 투표에서는 법적 구속력이 있는 PKI 인증서를 ID 카드 또는 스마트폰 USIM에 저장하여 네트워크로 투표에 참여한 유권자의 신분을 인증한다. 하지만 이 접근 방법은 공개키 인증서가 사용자 것임에 틀림이 없다는 것을 인증하지만 접속한 사용자가 본인인지를 인증하지는 못한다. 따라서 사용자가 본인의 인증서 또는 인증서가 저장되어 있는 스마트폰을 다른 사용자에게 위임하여 대리로 투표하는 것이 가능하다.

○ 매표 및 강권투표 방지

인터넷 기반의 모바일 투표에서 선거관리자가 유권자의 투표 행위를 감시하는 것은 사실상 불가능하다. 종이 투표 방식과 부분 전자투표 방식에서 유권자의 투표 행위는 지정된 장소에서 이루어지므로 선거관리자에 의한 감시가 가능하다. 인터넷 기반의 모바일 전자투표를 구현하기 위해서는 스마트폰 센서를 이용하여 지문, 얼굴 모양, 음성 등의 바이오 정보를 접목하여 제 3자의 감시 없이 본인만이 투표한다는 것을 입증할 수 있어야 한다.

○ 스마트폰에 적합한 모바일 ID

스마트폰은 모바일 플랫폼을 구성하는 대표적인 기기로 USIM 카드의 사용자 인증 정보인 IMSI (International Mobile Subscriber Identity) 토큰을 인증센터로 전송하여 스마트폰 소유자를 인증한다 [12]. USIM은 법적 효력을 갖는 절차에 의해서 등록되며 IMSI는 전화기마다 고유한 아이디로 사용자 신분 인증을 위한 용도로 사용될 수 있다. 하지만 USIM과 같은 토큰 기반의 인증 기법은 개인정보 도용 및 대리 인증의 위험이 있다. 스마트폰을 이용하여 모바일 투표, 전자현금 등 보다 많은 사회적 영역을 전자화하기 위해서는 프라이버시 보호와 대리 인증 문제를 동시에 해결할 수 있어야 한다.

다른 사용자에게 스마트폰을 빌려주어 본인 대신 인증을 받도록 하는 것을 대리 인증이라고 한다. 이를 방지하기 위해서는 사용자와 아이디가 물리적으로 연결되어야 하는데 사용자 바이오 데이터를 접목하는 것이 가장 이상적이다.

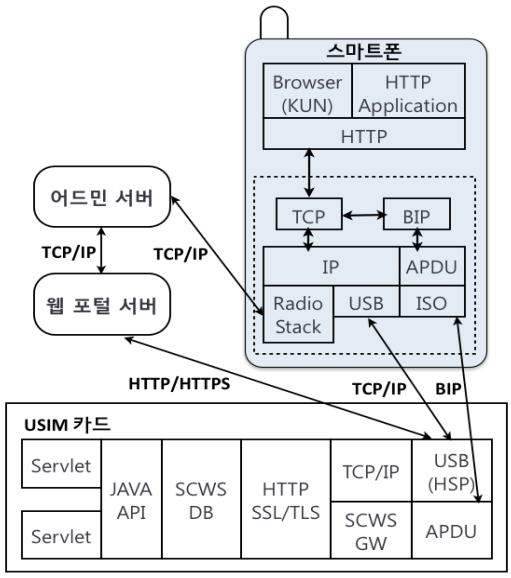
바이오 인식은 바이오 템플릿과 등록된 템플릿을 비교하여 사용자를 인증하는 것이다 [15, 18]. 바이오 정보로 사용되는 지문, 홍채, 음성은 개인 고유 정보이기 때문에 사용자와 아이디를 물리적으로 연결할 수 있다.

상기한 바와 같이 스마트폰 사용자 인증을 위한 용도로 사용될 디지털 ID는 USIM과 같이 법적 구속력을 가져야 하며 바이오 데이터와 같이 물리적으로 아이디를 연결할 수 있어야 한다.

4.2 USIM 기반의 법적 구속력 확보 [12, 13]

아이디는 본인임을 표현하는 식별자이다. 모바일 투표에 적용될 스마트폰용 모바일 ID는 법적 구속력이 있어야 한다. 주민등록증은 법적 효력을 갖는 인증 수단으로, 이를 발급받기 위해서는 본인이 직접 센터에 방문하여 본인임을 입증해야 한다. 모바일 ID가 법적 효력을 갖기 위해서는 주민등록증 발급과 유사한 신분 확인절차가 포함되어야 한다. PKI 기반의 인증서를 발급받을 때 최소 한 번 이상은 은행을 직접 방문하여 신분 확인을 하는 것과 마찬가지 이유이다.

법적 구속력 확보를 위해서 PKI 기반의 인증서를



(그림 2) USIM 서비스 접근

접목할 수도 있지만 스마트폰 USIM을 이용하는 것이 보다 더 효율적이다. USIM은 등록 센터를 방문하여 신분 인증이 되어야만 등록이 가능하고, USIM 카드 없이 전화를 사용할 수 없도록 법제화 되어 있다. 따라서 USIM은 개인의 법적인 신분을 표현하는 수단으로 활용 가능하다.

USIM 카드는 네트워크 접속 및 가입자 인증 소프트웨어 모듈로써 가입자 정보, 네트워크 정보, 인증 정보와 텍스트 메시지, 이메일, 폰 북 등의 개인 서비스 정보를 저장 및 관리한다. USIM 하드웨어는 RISC 방식의 32비트 프로세서까지 이용 가능하고 메모리는 운영체제 탑재를 위한 ROM, 응용 프로그램을 구동하기 위한 RAM, 응용 프로그램과 사용자 데이터를 저장하기 위한 EEPROM 또는 플래시 메모리로 구성된다. 플래시 메모리를 이용할 경우 이론적으로 상용화된 플래시 메모리 용량까지 개발이 가능하다.

USIM 카드는 프로그램 처리가 가능한 스마트카드이기 때문에 다양한 용도로 활용될 수 있다. (그림 2)는 웹 서버 기능을 USIM에 구현하여, HTTP 프로토콜을 지원하는 단말의 브라우저를 통해 USIM 서비스를 사용하는 방법을 보여준다. USB 또는 BIP 인터페이스를 이용하여 USIM 서비스에 접근이 가능하다. 서비스

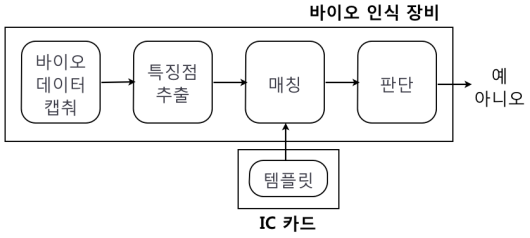
의 단말 플랫폼 의존성을 탈피하여 브라우저 기반의 서비스를 제공함으로써 USIM 이동성에 따른 서비스 호환의 한계를 극복할 수 있다.

USIM 카드는 3 장의 에스토니아 사례에서 살펴본 바와 같이 정부 주도로 사용자 아이디 정보, 디지털 서명 키, 보안 프로그램 모듈을 저장하여 원격으로 인증 서비스를 구현할 수 있게 커스터마이징되어야 한다. 모바일 투표에 필요한 법적 효력을 갖는 사용자 아이디를 만들기 위해서 USIM 카드를 접목하는 것은 매우 이상적인 솔루션이다.

4.3 바이오 정보를 접목한 사용자 인증

[15, 17, 18, 23]

USIM 만을 이용한 사용자 인증은 인터넷과 같은 비대면 공간에서 대리 인증 문제를 야기한다. 전자투표와 같이 원격 신분 인증이 요구되는 ID 기반의 사회적 시스템을 전자화 할 수 없다. 따라서 모바일 투표를 위한 스마트폰용 디지털 ID는 USIM과 더불어 사용자 바이오 데이터의 접목이 필요하다.

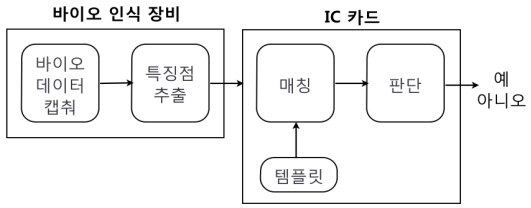


(그림 3) STOC (STore On Card) 바이오 인식

(그림 3)은 STOC 기반 바이오 인식 절차를 보여준다. 스마트카드에 사용자 바이오 정보를 저장하고 바이오 인식 장비에 접속시켜서 사용자 인식을 수행하는 방식이다.

(그림 4)는 MOC 기반 바이오 인식 기법을 보여준다. 바이오 인식 장비는 바이오 데이터 캡춰와 템플릿 생성 모듈로 구성된다. 스마트카드는 바이오 템플릿 보관과 매칭 기능을 수행한다.

바이오 인식 장비는 센서로서의 역할만 수행하고 나머지는 스마트카드에서 처리하는 모델로 데이터베



(그림 4) MOC (Match On Card) 바이오 인식

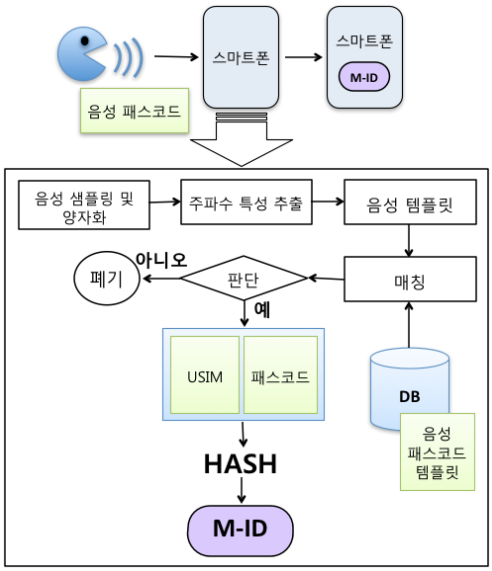
이스에 저장된 사용자 템플릿을 외부에 노출시키지 않기 때문에 STOC 모델보다 템플릿 노출의 위험이 적다.

바이오 인식 센서를 내장하고 있는 스마트폰은 바이오 인식 전 단계를 스마트폰에서 처리할 수 있다. STOC, MOC 기반 인식 시스템에서 발생할 수 있는 템플릿 노출 위험을 최소화할 수 있다. 스마트폰은 스마트카드와 달리 제조 단계에서 크기 및 무게를 규제하는 하드웨어 제약 사항이 없기 때문에 스마트폰 제조업체에서 바이오 인식 센서를 비롯하여 다양한 부가물을 설계에 반영하고 구현할 수 있다.

각종 센서와 프로그램 처리가 가능한 스마트폰은 기존의 PC 기반에서 상용화하기 어려웠던 여러 사회적 문제를 전자화할 수 있는 기반이 되고 있다. 바이오 정보가 접목된 모바일 ID를 내장한 스마트폰은 모바일 환경에서 사용자 인증을 위한 도구로 활용될 수 있다. 특히, 원격 전자투표와 같이 대리자에 의한 인증이 허용되지 않는 응용에서 본인임을 입증할 수 있는 용도로 사용될 수 있다.

지문 센서를 내장한 스마트폰은 그 보급률이 상대적으로 매우 낮아 실용적이지 못하고 얼굴 인식은 카메라 센서를 이용한 이미지 캡춰 지연 시간이 길어서 역시 실용적이지 못하다. 음성 인식의 장점은 모든 스마트폰이 음성 입출력 기능을 내장하고 있고 지연시간이 상대적으로 짧다는 것이다 [23].

화자 인증은 개인의 고유 음성 주파수 정보를 이용하여 개인 신분을 인식하는 기법이다. 스마트폰으로부터 입력된 음성 신호를 여러 패턴으로 분류하고 이 패턴들을 분석하여 입력 신호의 편차를 줄인다. 입력된 음성 신호는 음성 채널, 노이즈 등 다양한 소스를 포함하기 때문에 이들 신호 중에서 음성 채널을 구분하는 작업이 필요하다. 매칭 및 판단은 클래스로 분류



(그림 5) 모바일 음성 ID 생성

된 신호가 사용자 음성 채널로 적합한가를 결정한다 [17].

(그림 5)는 스마트폰을 이용한 사용자 인증에 적합한 모바일 ID 생성 단계를 보여준다. 모바일 ID는 스마트폰 USIM과 음성 패스코드를 이용하여 생성한다. 사용자는 본인만이 기억하는 패스코드를 발음으로 입력한다. 음성 패스코드 값만 변경함으로써 다양한 형태의 모바일 ID를 만들어 낼 수 있다. 입력된 음성 패스코드는 프레임 단위로 샘플링과 양자화를 거쳐서 디지털 신호로 변환된다. 프레임별로 사용자 고유 주파수를 찾아서 인증 벡터를 구성하고 템플릿으로 저장한다. 스마트폰에 저장된 음성 패스코드 템플릿과 입력된 템플릿을 비교하여 사용자 인증을 수행한다. 올바른 사용자이면 스마트폰에 삽입된 USIM으로부터 IMSI를 읽어서 인식된 패스코드와 함께 해쉬하여 모바일 ID를 생성한다.

5. 결 론

전자투표 방식은 인터넷 기반 투표와 기존 선거의 투표 및 개표 단계 중 일부만을 전자화하는 두 가지로 구분할 수 있다. 모바일 투표는 장소에 구애받지 않아야 하므로 선거의 전 단계를 전자화하는 인터넷 기반 투표가 가능해야 한다.

인터넷 기반 투표는 사용자의 투표권을 추적할 수 없는 믹스넷과 같은 채널이 준비되어야 하고 유권자에 의한 개별 검증이 가능해야 한다. 개별 검증을 위해서 발행하는 영수권은 유권자 이외의 다른 사람들이 유권자와 후보자를 연결할 수 없어야 한다.

에스토니아에서 지방 선거 및 의회 선거에 도입한 인터넷 기반 모바일 투표는 사용자 신분 인증을 위해서 PKI 기반의 공개키 인증서를 활용한다. WPKI 환경에서의 위험 요소와 대응 방안, USIM 카드를 이용한 사용자 인증 프로토콜을 제안하였다. 또한 ID-PKI 기반의 ID 카드를 이용한 전자투표 인프라를 스마트폰을 이용하는 모바일 투표로 적용 및 확장하는 방안을 제시하였다.

컴퓨터와 네트워크를 이용한 전자상거래에서 사용자 신분 확인은 PKI 기반의 인증서를 이용하는 것이 일반적이다. PKI는 전적으로 신뢰할 수 있는 인증기관을 두고 사용자 공개키 인증서를 배포 및 관리하는 시스템이다. 신분 확인이 이루어진 사용자만 디지털 인증서를 발급받기 때문에 법적 구속력을 갖고 전자상거래에서 구매자와 판매자 간의 거래 내용을 서명하여 법적 증거를 확보할 수 있다.

에스토니아 사례와 같이 PKI 인증서를 모바일 투표에 도입할 경우 대리 인증 문제와 매표 및 강권 투표에 대한 위험이 따르게 된다. 따라서 PKI 인증서를 대체할 수 있는 모바일 투표에 적합한 스마트폰용 모바일 ID가 요구된다.

선거에서 유권자 신분을 확인하는 절차는 투표권에 대한 법적 구속력을 부여하는 행위이다. 기존 선거에서 신분 확인은 투표소에서 선거관리인단이 유권자의 주민등록증과 유권자를 직접 대면하여 확인하는 것으로 이루어진다. 스마트폰을 이용한 모바일 투표에서 유권자는 장소에 관계없이 투표에 참여할 수 있어야 한다. 가상공간에서는 대면하여 신분 확인을 할 수 없기 때문에 모바일 ID는 도용, 대리, 위임의 위험이 높다. 투표에 응용되기 위해서 모바일 ID는 PKI 인증서와 같이 법적 구속력이 있어야 하고 사용자 바이오 데이터의 접목으로 가상공간에서 본인임을 입증할 수 있어야 한다.

법적 구속력을 확보하기 위해서 USIM 카드를 접목

하고, 대리 인증 위험을 최소화하기 위하여 사용자 음성 정보를 접목하는 것이 스마트폰용 모바일 ID의 실용화를 위해서 이상적이다. 또한 사용자 프라이버시 보호를 위하여 아이디 취소 및 재등록이 가능해야 하고 이를 위해서 음성 패스코드를 접목해야 한다.

모바일 ID 활용을 위해서는 PKI 기반의 CA와 같은 전적으로 신뢰할 수 있는 정부 주도의 ID 관리 센터가 만들어져야 한다. 전자 상거래 또는 전자투표와 같이 원격으로 신분을 인증해야 하는 응용에서 제 3자의 ID 인증 요구에 대해서 ID 센터와 ID 소유자 간에 원격으로 인증을 수행할 수 있어야 한다.

참 고 문 헌

[1] D. Evans, N. Paul, “Election Security: Perception and Reality,” IEEE S&P Magazine Jan/Feb, pp. 24-31, 2004.

[2] J. Tepandi, S. Vassiljev, I. Tsahhirov, “Wireless PKI Security and Mobile Voting,” IEEE Computer, Vol. 43, No. 6, pp. 54-60, 2010.

[3] Beroggi, “Secure and Easy Internet Voting,” Computer, Feb. 2008, pp. 52-56.

[4] D. L. Dill and D. Castro, “Point/Counterpoint: The U.S. Should Ban Paperless Electronic Voting Machines,” Commmunications of the ACM, vol. 51, no. 10, pp. 29-33, 2008.

[5] N. Paul and A.S. Tanenbaum, “Trustworthy Voting: From Machine to System,” Computer, May 2009, pp. 23-29.

[6] Estonian National Electoral Committee, “General Description of the E-Voting System,” 2004; www.vvk.ee/public/dok/Yldkirjeldus-eng.pdf.

[7] D. Chaum, “Secret-Ballot Receipts: True Voter-Verifiable Elections,” IEEE S&P Magazine Jan/Feb, pp. 38-47, 2004.

[8] D. Chaum, “Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms,” Communications of the ACM, Vol. 24, No. 2, pp. 84-88, 1981.

[9] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta, “A Practical Secret Voting Scheme for Large Scale Elections,” In Advances in Cryptology, Proceedings of AUSCRYPT’92, 1992.

[10] 정연정, “미국의 전자투표,” 한국정치학회, 한국정치학회보, 제39집, 제3호, 2005.

[11] 이광우, 이윤호, 원동호, 김승주, “전자투표 신뢰성 향상을 위한 유권자 검증 영수증 발급 기술,” 한국정보보호학회, 정보보호학회논문지, 제16권, 제4호, 2006.

[12] The 3rd Generation Partnership Project, “Characteristics of the Universal Subscriber Identity Module (USIM) Application,” technical specification 3GPP TS 31.02.

[13] P. Urien, “Convergent identity: Seamless OPENID services for 3G dongles using SSL enabled USIM smart cards,” IEEE CCNC, pp. 830 - 831, 2011.

[14] E. Maler, D. Reed, “The Venn of Identity: Options and Issues in Federated Identity Management,” IEEE Security & Privacy, Vol. 6, No. 2, 2008.

[15] C. Vivaracho-Pascual, J. Pascual-Gaspar, “On the Use of Mobile Phones and Biometrics for Accessing Restricted Web Services,” IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, pp. 1-10, 2011.

[16] Want, “iPhone: Smarter Than the Average Phone,” IEEE Pervasive Computing, Vol. 9, No. 3, pp. 6-9, 2010.

[17] P. Campbell, “Speaker Recognition: A Tutorial,” Proceedings of the IEEE, Vol. 85, No. 9, 1997.

[18] N. Ratha, J. Connell, R. Bolle, “Enhancing security and privacy in biometric-based authentication systems,” IBM Systems Journal, Vol. 40, No. 3, pp. 614 - 634, 2001.

[19] Baltic WPKI Forum; http://wpki.eu.

[20] M. Assora, J. Kadirire, and A. Shirvani, “Using WPKI for Security of Web Transaction,” Proc. 8th Int’l Conf. E-Commerce and Web Technologies (EC-Web 07), LNCS 4655, Springer, 2007, pp. 11-20.

[21] M. Hassinen, K. Hyppönen, and E. Trichina, “Utilizing National Public-Key Infrastructure in Mobile Payment Systems,” Electronic Commerce Research and Applications, vol. 7, no. 2, 2008, pp. 214-231.

[22] R. Oppliger, R. Hauser, and D. Basin, “SSL/TLS Session Aware User Authentication,” Computer, Mar. 2008, pp. 59-65.

[23] Haizhou Li, Kar-Ann Toh, Liyuan Li, Advanced Topics in Biometrics, World Scientific, 2011.

◐ 저 자 소 개 ◑

윤 성 현

1992년 고려대학교 컴퓨터학과(이학사)
1994년 고려대학교 컴퓨터학과(이학석사)
1997년 고려대학교 컴퓨터학과(이학박사)
1998년~2002년: LG전자 중앙연구소 선임연구원
2002년~현재 백석대학교 정보통신학부 조교수
관심분야 : DRM, 전자투표 등
E-Mail : shcrpt@gmail.com