정 보 보 호 학 회 지
제24권 제4호, 2014. 8

모바일 기기 기반의 다중요소 인증기술 국제 표준화 동향

김 근 옥*, 정 영 곤**, 심 희 원***, 강우진****

요 약

오늘날 사람들은 장소와 시간의 제약 없이 인터넷에 접속하여 정보검색, 인터넷뱅킹, 온라인쇼핑 등의 다양한 서비스를 제공받을 수 있다. 특히 모바일 기기를 활용한 서비스가 증가하면서 모바일 기기를 통한 다양한 인증기술이 선보이고 있는 실정이다. 최근에는 전자거래의 보안위협에 대응하기 위해 고위험 거래에서는 하나 이상의 인증요소를 결합한 다중요소 인증기술을 권고하기도 한다. 이에 본 논문에서는 최근 ITU-T SG17에서 진행 중인 모바일 기기를 활용한 다중요소 인증기술 관련 국제 표준화 동향을 살펴본다.

Ⅰ. 서 론

최근의 인터넷 환경은 점점 더 교묘해지는 해킹 기술로 인해 단일요소 인증기술로는 다양하고 지능적인 해킹위협에 효과적으로 대응하기 어려워지고 있는 현실이다. 일반적으로 사용자인증을 위해서는 패스워드, SMS인증, 일회용비밀번호, 디지털인증서 등의 다양한 인증기술을 사용하고 있다. 하지만 공격자는 금전적 이득을 취하기 위해 다양한 방법으로 인증정보의 해킹을 시도하고 있어, 단일요소 인증기술만을 적용한 경우 해당 정보 유출에 따른 큰 위험을 초래할 수 있다. 최근에는 이러한 단일요소 인증기술을 보완하기 위한 방법으로 두 개 이상의 단일요소 인증기술을 결합한 다중요소 인증기술에 대한 요구가 증가하고 있다. 미국 연방금융기관검사위원회(FFIEC)의 '인터넷뱅킹 환경의 인증 가이드라인' [1] 과 싱가포르 통화감독청(MAS)의 '전자금융 위험관리 가이드라인' [2] 에서는 고위험거래에서는 멀티팩터 인증을 권고하고 있다.

2012년 8월 ITU-T SG17(정보보호)에서는 모바일기기 기반의 멀티팩터 인증에 대한 표준화를 시작하여 올해 하반기 최종 승인을 목표로 표준안을 개발중에 있다.

본 논문에서는 모바일기기를 활용한 다중요소 인증기술에 대한 국제 표준화 동향을 살펴본다.

본 논문의 구성은 2장에서 사용자 인증기술과 관련하여 단일요소 인증기술을 구분하고 두 개 이상의 단일요소를 결합한 다중요소 인증기술을 설명한다. 3장에서는 다중요소 인증기술의 국제 표준화 동향을 살펴보고 마지막 결론으로 4장에서 다중요소 인증기술의 표준화 전망을 기술한다.

Ⅱ. 인증기술 분류

2.1. 개요

인터넷서비스의 비대면 특징으로 인해 사용자가 허가된 사용자임을 입증하는 사용자인증이 매우 중요하다. 사용자인증 기술을 인증요소에 따라 분류하면 소지기반, 지식기반, 특성기반으로 분류할 수 있다[3].

〔표 1〕 인증 요소의 분류

인증요소	설 명
소지기반	사용자가 소유하고 있는 인증요소
지식기반	사용자만이 알고 있는 인증요소
특성기반	사용자의 특성 정보 인증요소

본 연구는 미래창조과학부의 지원을 받는 방송통신표준기술력향상사업의 연구결과로 수행되었음
* 금융보안연구원 인증기술팀 (kko@fsa.or.kr)
** 금융보안연구원 인증기술팀 (ygjung@fsa.or.kr)
*** 금융보안연구원 인증기술팀 (hwshim@fsa.or.kr)
**** 금융보안연구원 인증서비스본부 (hanull@fsa.or.kr)

이밖에도 사용자마다 다른 입력패턴의 차이, 전자적인 서명필체, 모바일 기기를 활용한 사용자의 위치정보를 이용하는 등의 인증기술이 위에서 분류에 포함될지, 새로운 인증요소로 분류될지는 계속 논의 중에 있는 상황이다.

2.2. 단일요소 인증기술

단일요소 인증기술이란 위에서 정의한 사용자 인증요소 중에 하나의 인증요소만 활용하여 사용자 인증을 하는 방식이다.

2.2.1. 소지기반 인증

소지기반 인증요소(What you have)는 사용자가 소유하고 있는 요소를 이용하여 사용자를 인증하는 방식이다. 소지기반 인증 요소로 사용되는 대표적인 인증기술로는 OTP(일회용비밀번호), 스마트카드, 보안토큰(HSM) 등이 있다. 인터넷뱅킹에서 자금이체 시 최종 사용자 인증수단으로 사용자가 소지하고 있는 OTP를 입력하여 정당한 사용자가 거래를 지시하였음을 확인한다. 일반적으로 소지기반의 인증요소는 보안성으로 인해 대면에 의한 본인확인 후 발급되며, 인증매체의 소지 및 비용 등의 사용자 편의성 이슈가 존재한다.

2.2.2. 지식기반 인증

지식기반 인증요소(What you know)는 사용자가 알고 있는 요소를 통해 사용자를 인증하는 방식이다. 지식기반 인증 요소로 사용되는 인증기술의 예로는 비밀번호, PIN 등이 있다. 사용자가 웹사이트 로그인시 사용자의 ID와 사용자만 알고 있는 비밀번호를 입력하여 인증함으로써 사용자 본임임을 확인한다. 일반적으로 지식기반의 인증요소는 온라인상에서 편리한 사용자 인증기술로 널리 사용되고 있다.

2.2.3. 특성기반 인증

특성기반 인증요소(What you are)는 사용자가 가지고 있는 고유한 특성을 이용하여 사용자를 인증하는 방법이다. 특성기반 인증요소로 사용되는 인증기술의 예로는 지문, 목소리, 홍채 등이 있다. 예를 들어, 비밀금고 출입시 사용자는 등록한 지문을 입력하여 사용자 본인임을 확인할 수 있다. 특성기반 인증기술은 보안성이 뛰어난 인증기술이기는 하나, 특성정보 노출에 따른 프라이버시 이슈 등으로 인해 접근제어 용으로 주로 사용되고 있다.

2.2.4. 기타 인증요소

위에서 분류하는 세 가지 인증요소 외에 최근에는 전자적인 서명필체, 위치정보 등의 인증기술이 사용되어지고 있다. 사용자 스마트폰의 GPS 기능을 활용하여 사용자의 위치를 확인하여 유효한 경우에만 서비스를 제공하는 등의 방법으로 사용되고 있다. 이러한 인증기술 들은 최근 기술의 발달로 소지기반, 지식기반, 특성기반 인증요소 외에 다양하게 사용자를 확인할 수 있는 인증요소가 개발되어 사용하고 있다.

2.3. 다중요소 인증기술

다중요소 인증기술은 각각의 단일요소 인증기술을 두 가지 이상의 인증요소를 결합하여 사용자를 인증하는 방법을 의미한다. 포털, 금융, 게임 사이트 등의 국내 온라인 서비스에서 대표적으로 사용되는 다중요소 인증기술로는 사용자의 지식기반 인증요소인 비밀번호와 소지기반 인증요소인 OTP의 두 가지의 인증요소를 이용하는 것을 예로 들 수 있다.

다중요소 인증기술은 하나의 인증요소가 해킹에 의해 유출 또는 탈취 되더라도 이와 독립적인 다른 인증요소에 의해 안전하게 사용자 인증을 제공할 수 있기 때문에 단일요소 인증에 비하여 보안성을 향상시킬 수 있다.

Ⅲ. 모바일 기기 기반의 다중요소 인증기술 개요

3.1. 개요 및 특징

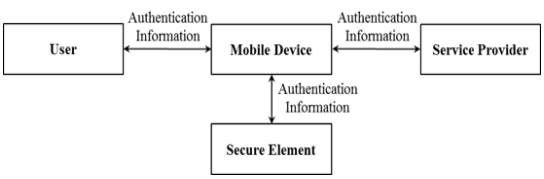
최근 모바일 기기가 발달함에 따라 모바일 기기를 활용하여 사용자 편의성을 향상시킨 인증기술이 등장하고 있다. 예를 들어, USIM, 현금 IC카드와 NFC기능이 내장된 모바일 기기를 활용한 일회용비밀번호(OTP), 공

인인증서 등의 서비스가 이에 속한다. 또한 인터넷뱅킹을 통한 자금이체 시 등록된 휴대폰번호로 전화를 걸어 추가인증을 하는 등의 2채널 인증도 모바일 기기를 활용한 인증기술이라고 하겠다.

전자금융이 발달한 국내에서는 이러한 인증기술의 개발이 더욱 가속화됨에 따라, 금융보안연구원에서는 2012년 8월 ITU-T SG17(정보보호)에 모바일기기 기반의 다중요소 인증에 대한 표준안 〔4〕 을 제안하였다.

해당 표준안에서는 기본적으로 모바일 기기를 활용하여 인증정보를 생성하고 이를 통해 다중요소 인증을 제공할 수 있는 서비스모델을 제시하고 있다.

인증정보를 생성하는 모바일 기기는 사전에 인증서버에 안전한 방법으로 등록됨을 가정하고 있기 때문에 다양한 요소의 인증기술들이 모바일 기기를 활용하여 인증정보를 생성할 경우 소지기반 인증요소의 특징을 갖게 된다. 예를 들어, [그림 1]와 같이 사용자가 지식기반 또는 특성기반의 인증정보를 모바일 기기에 전달하면, 모바일 기기는 모바일기기 자체적으로 또는 보안요소(secure element)를 이용하여 소지기반의 특성을 추가한 새로운 인증정보를 생성하여 이를 통해 사용자 인증을 하게 된다.



〔그림 1〕 모바일 기기 기반의 다중요소 인증기술의 개요

그렇기 때문에 모바일 기기 기반의 다중요소 인증기술은 모바일 기기를 통해 생성된 소지기반 특성의 인증요소 이외에 하나 이상의 요소 인증기술을 함께 전달함으로써 다중요소 인증이 가능하다.

3.2. 보안 요구사항

모바일 기기 기반의 다중요소 인증을 제공하기 위해서는 다음의 일반적인 요구사항과 각 객체별 보안요구사항을 만족해야 한다.

3.2.1. 일반사항

다중요소 인증은 ITU-T X.1254에 있는 객체인증보증 프레임워크 보안 요구사항을 만족하여야 한다.

다중요소 인증은 ITU-T X.1254에 있는 등록, 신원관리, 인증의 실행절차 요구사항을 만족하여야 한다.

다중요소 인증에서의 각 객체에 대한 신원은 ITU-T X.1254에 있는 등록절차에 의해 확인되어야 한다.

다중요소 인증에서의 각각 인증 요소의 기밀성은 ITU-T X.1254에 있는 비밀관리 절차에 따라 관리되어야 한다.

다중인증 메커니즘은 사용자 인증을 위한 두 개 이상의 서로 다른 형태의 인증요소를 제공하여야 한다.

다중인증 메커니즘은 다중요소 인증 시 서버 인증, 무결성, 기밀성을 제공해야 한다.

다중인증 메커니즘은 재생공격에 대비할 수 있는 모바일 기기나 보안 요소를 사용한 소지기반의 인증 정보를 생성하여야 한다.

다중요소 메카니즘은 사용자로부터 제공되어 전송되거나 저장되는 바이오정보에 대한 프라이버시 보호가 요구된다.

3.2.2. 모바일기기

모바일기기는 안전한 방법으로 서비스제공자에 등록되어야 한다.

모바일기기는 거래 세부내역을 확인하는 등의 사용자의 명시적인 확인에 의해 인증정보가 생성되어야 한다.

모바일기기는 인증정보를 생성하는데 사용된 정보를 사용 후에 즉시 삭제하여야 한다.

모바일기기 내의 모듈은 보안 소프트웨어를 사용하여 악성프로그램에 의해 침해되거나 복제되는 위협 등으로부터 보호가 되어야 한다.

모바일기기의 도난이나 분실에 대비하여 비인가자의 접근을 차단하는 지문 인증, PIN 등과 같은 접근통제 기능의 제공이 요구된다.

모바일기기는 타임스탬프를 포함하여 거래세부정보로부터 디지털 포렌식을 위한 기록이 요구된다.

3.2.3. 보안요소

접근통제 기능이 있는 보안요소는 비 정상적인 접근 시도에 대한 임계치를 설정해야 한다.

보안요소내에 저장된 비밀정보(개인키, 사용자와 서비스제공자간에 미리 공유된 비밀키 등)은 보안요소 외부로 유출이 되어서는 안된다.

보안요소는 인증정보의 생성을 분명한 사용자의 확인에 의해 안전하게 생성하여야 한다.

가상 보안요소(virture SIM 등)는 하드웨어 기반의 보안요소와 동등한 보안을 유지해야 한다.

3.2.4. 서비스 제공자

서비스 제공자는 소지기반 인증정보가 미리 등록된 모바일기기로부터 전송되었음을 확인하고 사전에 등록된 사용자 소유의 모바일기기에서 생성되었음을 입증하여야 한다.

서비스 제공자는 HSM과 같은 안전한 방법을 사용하여 비밀키의 유출에 대비해야 한다.

서비스 제공자는 서비스에 사용되는 용어와 사용방법에 대해 사용자에게 공지하거나 교육을 제공하는 것이 필요하다.

서비스 제공자는 데이터에 대한 무결성을 보장하고 타임스템프를 포함하여 거래 세부정보로부터 디지털 포렌식을 위한 기록이 필요하다.

Ⅳ. 모바일 기기 기반의 다중요소 인증 메커니즘

해당 표준안에서는 모바일 기기 기반의 다중요소 인증 메커니즘을 객체, 연산, 서비스모델, 프로토콜로 정의하고 있다.

4.1. 객체

사용자: 사용자는 지식기반 인증 요소(패스워드, PIN 등)나 생체기반 인증 요소(지문, 홍체 등)을 가지고 있고, 디바이스, 모바일 기기등의 소지기반 인증요소를 생성할 수 있는 기기를 소유하고 있다.

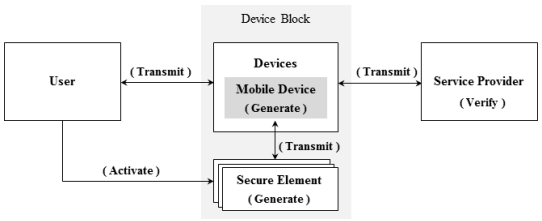
기기: 인증정보를 생성하고 전송하는 모바일 기기와 전송기기의 집합이다. 인증정보를 생성하기 위해 사용되는 최소한 한 개의 모바일 기기가 있어야 하고 인증정보를 전송하기 위한 최소한 한 개의 전송기기가 있어야 한다. 이 메커니즘에서는 모바일 기기가 전송기기의 역할도 함께 수행할 수 있다. 모바일 기기는 사용자가 항상 소지하여야하고 소지기반의 인증정보를 생성할 수 있다. 전송기기는 온라인 서비스에 접속하여 서비스 제공자와 통신이 가능한 기기로 PC, 스마트폰 등이 될 수 있다.

보안요소: IC칩이나 보드 칩으로 소지기반의 인증정보를 안전하게 생성할 수 있다. 사용자와 서비스제공자간에 미리 공유된 비밀키를 안전하게 저장하고 이 비밀키로 안전하게 소지기반의 인증정보를 계산할 수 있다.

서비스제공자: 서비스 제공자는 사용자의 모바일기기로부터 전송된 인증정보를 검증한다.

4.2. 연산

[그림2]은 구성요소사이에서의 운영을 보여준다. 기기블록은 가상의 블록으로 모바일기기, 전송기기, 보안요소를 포함한다. 사용자는 인증정보를 모바일기기에 입력하거나 사람이 인지할 수 있는 방법으로 모바일기기에서 전달받는다. 또한 사용자는 보안요소를 동작시켜 모바일기기를 통해 인증정보를 전달받을 수 있다. 모바일기기와 보안요소는 소지기반 인증정보를 생성하는 역할을 하고 전송기기는 서비스제공자에게 인증정보를 전송하는 역할을 한다.



〔그림 2〕 메커니즘에서 사용하는 주요 연산

전송(Transmit) : 인증정보를 디바이스로 전송하거나 전송받는다. 사용자와 디바이스 사이에서는 사람이 인지할 수 있는 다양한 방법으로 전송한다. 디바이스와 보안요소 사이에서는 블루투스, NFC 등의 기술을 이용하여 전송한다. 디바이스와 서비스 제공자 사이에서는 LAN, WIFI 등을 이용하여 전송한다.

활성화(Activate) : 소지기반의 인증정보를 생성하기 위해 보안요소를 작동시키는 것으로, 전원을 동작시키거나 패스워드, 지문 등의 입력으로 동작시킬 수 있다.

생성(Generate) : 모바일기기와 보안요소는 소지기반의 인증정보를 생성할 수 있다.

검증(Verify) : 디바이스로부터 전송된 인증정보를 검증하는 것으로 서비스 제공자는 멀티 인증정보를 검증하여 사용자를 인증할 수 있다.

4.3. 서비스 모델

모바일 기기 기반의 다중요소 인증서비스 모델은 인증정보를 생성하는 모바일 기기의 특성에 따라 3가지 기본 모델을 제시하고 있으며, 서비스 방식에 따라 다양한 방식으로 결합하여 서비스가 가능하다.

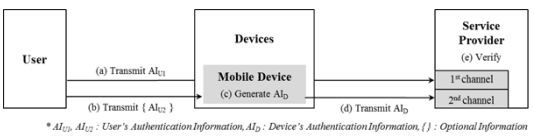
첫 번째 서비스 모델은 모바일 기기에서 인증정보를 생성하는 ‘Mobile device with multi-channel’ 모델로, 모바일 기기의 위변조 등의 보안위협에 대한 보안성을 담보하기 위해여 별도의 채널을 통해 두 번째 요소의 인증이 수반되어야 한다. 두 번째 서비스 모델은 모바일 기기와 보안요소(secure element)를 활용하여 인증정보를 생성하는 ‘Mobile device with secure elements’모델로, 비밀정보의 저장 및 인증정보 생성을 안전한 보안요소(secure element) 내부에서 하기 때문에 보안성이 우수한 모델이다. 다만, 악성코드 등에 의해 의도하지 않은 인증정보 생성의 우려가 존재하기 때문에 안전한 접근제어를 제공해야 한다. 마지막으로 세 번째 모델은 전용기기를 통해 인증정보를 생성하는 ‘Stand-alone mobile device’ 모델이 있다. 전용기기를 통해 생성한 인증정보는 전자거래 채널에 사용자가 직접입력하거나 통신을 통해 전달이 가능하다. 각각의 서비스 모델에 대한 자세한 설명과 프로토콜은 아래와 같다.

4.3.1 다중채널 모델

다중채널 모델(Mobile device with multi-channel)은 등록된 모바일 기기에서 소지기반의 인증정보를 생성하는 모델로, 모바일 기기가 해킹 등으로 인해 오염된 경우 모바일 기기를 통해 생성된 인증정보도 오염될 가능성이 존재하므로 별도의 채널을 통해 2번째 요소 인증을 제공하는 다중채널·다중요소 인증모델이다.

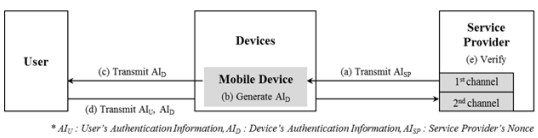
전자금융사기예방 서비스의 일환으로 단말기지정서비스를 예로 들어보면, 미리 지정된 모바일 기기로 인터넷뱅킹에 로그인할 경우를 소지기반의 1번째 요소인증으로 본다면, 이 경우 별도의 채널을 통해 지식 또는 특성기반의 2번째 요소 인증을 수행해야만 안전한 멀티요소 인증이 될 수 있다. 지정된 모바일 기기가 악성코드에 의해 오염되었더라도 별도의 채널을 통해 2번째 인증을 하기 때문에 보다 안전한 인증서비스를 제공할 수 있기 때문이다.

해당 모델은 인증정보를 생성·전달하는 방식에 따라 [그림 3]의 일방향 모델과 [그림 4]의 양방향 모델로 구분할 수 있다.



〔그림 3〕 일방향 다중채널 모델

일방향 다중채널 모델은 사용자가 모바일 기기를 활용하여 인증정보를 생성한 후, 서비스 제공자에게 전달하는 일반적인 모델이다.

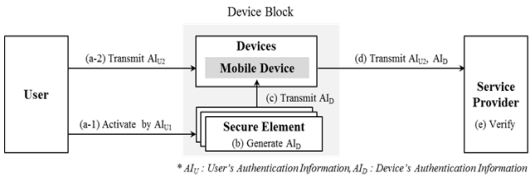


〔그림 4〕 양방향 다중채널 모델

양방향 모델은 SMS OTP 서비스와 같이 서비스제공자로부터 인증정보 생성에 필요한 정보를 전달받아 인증하는 모델이다.

4.3.2 보안요소 모델

보안요소 모델(Mobile device with secure elements)은 모바일 기기와 보안요소(secure element)를 활용하여 안전하게 소지기반 인증정보를 생성하는 모델로, 모바일 기기가 해킹 등으로 인해 오염된 경우라도 보안요소를 통해 생성된 인증정보는 위변조에 대응가능하기 때문에 동일한 채널을 이용한 다중요소 인증이 가능한 모델이다.



〔그림 5〕 보안요소 모델

보안요소 모델의 대표적인 예로는, USIM이나 IC카드 기반 일회용비밀번호(OTP)나 공인인증서를 들 수 있다.

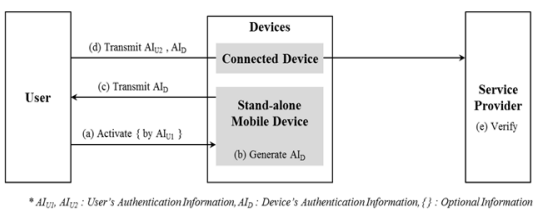
스마트폰에 장착된 USIM이나 스마트폰과 통신(NFC 등)이 가능한 IC카드 등의 보안요소에 인증정보 생성을 위한 비밀정보를 미리 발급받아 저장한다. 사용자는 거래정보 등을 모바일 기기를 통해 보안요소에 전달하고, 보안요소 내부에서 안전하게 생성된 소지기반의 인증요소를 1번째 인증을 수행한다. 이 경우 2번째 인증요소는 동일한 채널로 전달되어도 안전한 인증서비스를 제공가능하다.

다만, 보안요소 모델은 모바일 기기의 오염에 의해 의도하지 않은 인증정보를 생성할 가능성이 존재하므로, 명시적인 사용자의 개입에 의해 인증정보가 생성되는 능동형 접근제어 기능을 제공해야 한다.

4.3.3 전용기기 모델

전용기기 모델(Stand-alone mobile device)은 전용기기를 활용하여 안전하게 소지기반 인증정보를 생성하는 모델로, 전용기기가 위변조에 대응 가능하기 때문에 전용기기를 통해 생성된 인증정보는 위변조에 대응가능하다. 그렇기 때문에 동일한 채널을 이용한 다중요소 인증이 가능한 모델이다.

대표적인 전용기기 모델은, OTP 토큰이 있다. 전용 OTP 토큰을 통해 생성한 인증정보를 인터넷뱅킹에 입력 시 동일한 채널을 통해 2번째 요소 인증을 수행하여도 안전하게 인증서비스를 제공 가능하다.



〔그림 6〕 전용기기 모델

Ⅴ. 결론

모바일 기기의 활용도가 높아짐에 따라, 모바일을 활용한 다양한 방법의 인증기술 또한 요구되고 있다. 이에 본 논문에서는 최근 ITU-T SG17에서 진행중인 모바일 기기를 활용한 다중요소 인증기술 동향을 살펴보았다. 일반적으로 사용자가 소지하고 다니는 모바일 기기를 소지기반 인증요소로 활용하여 다중요소 인증을 제공할 수 있다면 전자거래의 안전성을 높일 수 있을 것이다. 해당 표준에서는 인증정보를 생성하는 모바일 기기의 특성에 따라 3가지 기본 모델을 제시하고 있고 서비스 환경에 맞도록 기본 모델을 적절히 결합하여 다양한 환경에 적용이 가능할 것으로 기대된다.

참 고 문 헌

[1] 금융보안연구원, “전자금융 新인증기술 연구보고서”, 금융보안연구원 연구보고서, 금보원 2011-01, Mar 2011.

[2] FFIEC, Supplement to Authentication in an Internet Banking Environment, Jun. 2011.

[3] MAS, Internet banking and technology risk management guidelines, Version 3.0, 2 June 2008.

[4] ITU-T, “X.sap-8: Multi-factor authentication mechanisms based on a mobile device, draft, Jan.2014.

〈저 자 소 개〉

김 근 옥 (Kim, Keun-ok)
정회원

2004년 2월 : 성균관대학교 전자전기 컴퓨터공학과 석사
2011년 8월~현재 : 성균관대학교 전자전기 컴퓨터공학과 박사과정
2001년 3월~현재 : 금융보안연구원 인증기술팀 선임연구원
관심분야 : OTP, 암호이론, 정보보호

정 영 곤 (Jung, young-gon)
정회원

2010년 2월 : 순천향대학교 정보보호학과 학사
2012년 2월 : 순천향대학교 정보보호학과 석사
2012년 1월 ~ : 금융보안연구원 인증기술팀 주임연구원
관심분야 : OTP, PKI, 정보보호

심 희 원 (Shim, hee-won)
정회원

2000년 2월 : 홍익대학교 전자계산기학과 석사
2011년 8월 : 전남대학교 정보보호학과 박사
2006년 12월~현재 : 금융보안연구원 인증기술팀 팀장
관심분야 : PKI, OTP, 네트워크 보안, 암호이론

강 우 진 (Kang, woo-jin)
정회원

1992년 2월 : 연세대학교 중어중문학과 학사
2006년 10월~현재 : 금융보안연구원 인증서비스본부 본부장
관심분야 : OTP, 네트워크 보안