카드사 대체 인증기술 보안성 비교 분석

(보안연구부 보안기술팀 / 2016.4.21)

1. 개요

o '14년 온라인 카드결제시 공인인증서 의무 사용 폐지[1], 온라인 간편결제 활성화[2] 대책 발표 이후 공인인증서를 대체하기 위한 기술이 지속적으로 개발되고 있음

- 다만, 대체 인증기술에 따라 이용 환경(단말기, 운영체제 등)의 제약과 절차상 요구하는 정보의 차이가 존재

o 본 보고서에서는 카드사 서비스 이용(서비스 가입, 결제* 등) 시 제공되는 공인인증서 기반 본인인증 서비스를 대체하는 인증기술의 보안성을 비교 분석함

* 결제 시 인증이 아닌 특정금액 이상 결제하여 추가인증이 필요한 경우

- 제공 예정인 서비스의 경우 일부 내용이 변경되어 출시될 수 있음

2. 상세 분석

□ 신용(체크)카드인증

o 소지하고 있는 카드의 정보(카드번호, 유효기간, 비밀번호, CVC[3])를 입력하여, 해당 카드를 본인이 소지하고 있는지 여부를 확인하는 서비스임

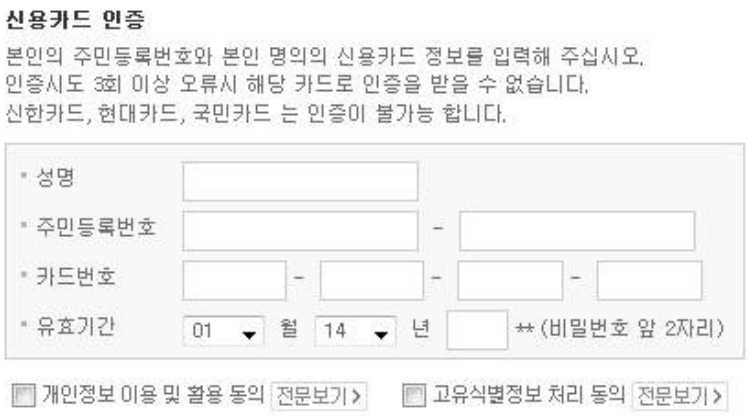
- **(편의성)** 카드만 소지함으로써 편리함

o **(위험성)** 카드 정보를 사진, 텍스트로 전달하는 등 입력정보가 쉽게 노출될 수 있어 타인이 쉽게 인증 할 수 있음

※ 노출위험성이 높아 단독으로 사용하지 않고, 다른 인증방식과 함께 이용

1) 금융위원회, 온라인 카드결제시 공인인증서 의무 사용 폐지를 위한 「전자금융감독규정 시행세칙」개정, 2014.5.19.
2) 금융위원회, 전자상거래 결제 간편화 방안, 2014.7.28.
3) CVC(Card Validation Code) : 카드 유효성 검사 코드로 카드의 고유번호를 의미

< 신용카드 본인확인 서비스(자료:구글 이미지) >



□ ARS(자동응답시스템)/SMS 인증

o ARS 혹은 SMS로 이용자에게 전달되는 인증번호(임의 생성된 숫자 값 등)를 입력하여 이동통신사업자의 서비스 이용 여부를 통해 본인임을 인증하는 서비스임

- **(편의성)** 휴대폰 기종(피처폰, 스마트폰 등)을 구별하지 않고 이용 가능
- **(보안성)** 최소한의 개인정보*(성명, 휴대폰번호, 생년월일 등)로 본인 여부 및 휴대폰 보유 여부를 확인하여 보안 강화

  * 서비스 기관마다 개인정보 입력 요구사항이 다르며, 입력 정보 일치 여부 확인, 개인 식별 가능 여부 등 기능적 차이가 존재

o **(ARS 인증)** 인증전화를 거는 주체에 따라 인증방식이 2가지로 구별됨

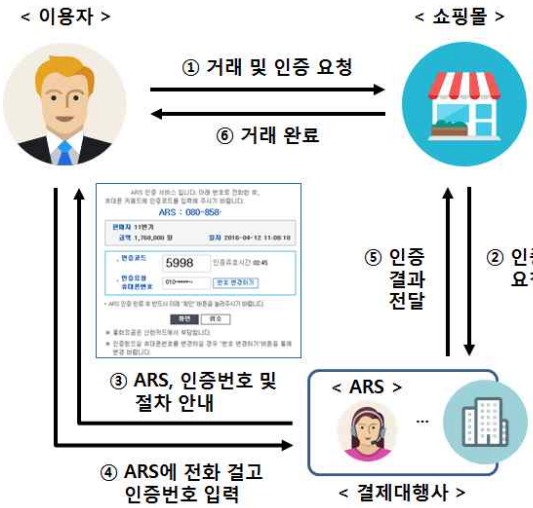
- **(인바운드, In-bound)** 화면에 출력되거나 문자로 전송받은 인증번호를 특정 전화번호(거래건마다 부여되는 가상 전화번호)로 이용자가 직접 전화를 걸어 인증번호를 입력하여 인증하는 방식

  ※ 이용자가 미리 지정한 전화번호로 발신하였을 때만 인증 가능

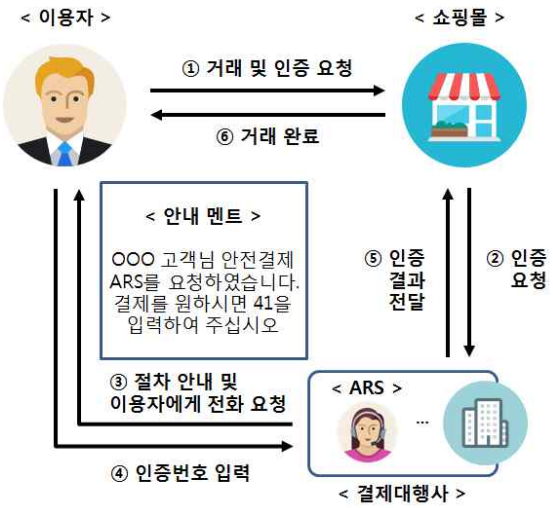
- **(아웃바운드, Out-bound)** ARS인증을 요청하면 이용자에게 전화가 수신되고, 이용자는 수신된 자동음성의 안내에 따라 인증번호를 입력하여 인증하는 방식

  ※ 이용자가 사전에 지정한 전화번호로만 수신 가능

< 인바운드 방식 절차 >

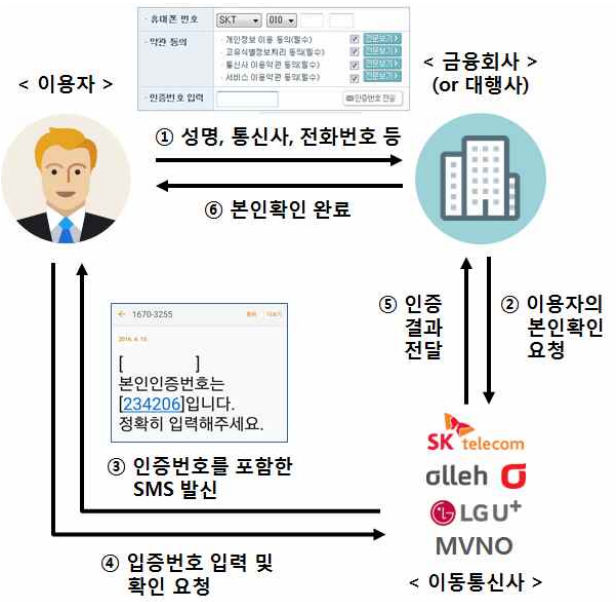


< 아웃바운드 방식 절차 >



o **(SMS 인증)** 가입자 명의의 휴대폰으로 인증번호를 포함하는 SMS가 수신되면, 이용자는 인증번호를 입력하여 본인임을 확인함

< 본인확인 서비스 인증 절차 >



o **(위험성)** 통신사 부가서비스(착신전환 등), 악성코드(원격 제어, SMS 탈취) 통신장비 조작 등을 통한 인증정보 탈취 위협이 존재함

- **(착신전환)** 부가서비스 혹은 프로그램에 의한 착신전환으로 본인 단말기 이외의 단말기에서 인증 수행 가능
- **(악성코드)** 원격 제어 기능으로 임의의 인증을 수행 및 SMS 탈취 가능

- **(통신장비 조작)** 이동통신사의 기지국, 사설교환기, 회선교환기(PBX) 등의 통신 장비를 조작하는 경우 대상 범위의 기기에 대한 발신번호 조작, 착신 조작 등 악용 가능

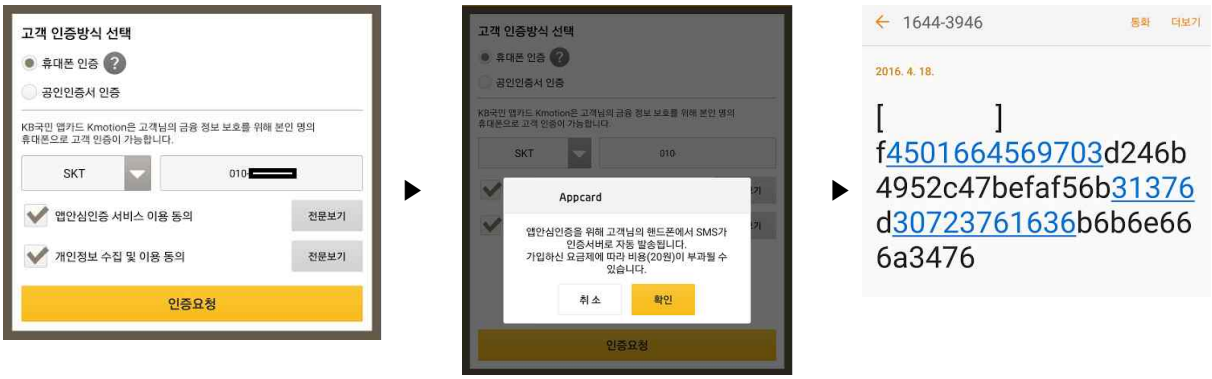
※ 단, 통신장비 조작은 장소적 제약이 발생하여, 대상이 한정적

□ 휴대폰 인증(앱안심인증)

o ARS 인증보다 보안을 강화한 것으로 이동통신사에 등록된 기기여부를 확인하는 인증절차로 본인 명의 휴대폰 여부를 확인하는 서비스임

- **(편의성)** 개인정보 입력 절차 생략
- **(보안성)** 이동통신사에 등록된 기기인지 확인하는 과정을 통해 등록된 기기 이외에서 인증이 불가능하도록 인증 강화

< 휴대폰 인증(앱안심인증) 절차 >



o **(위험성)** 원격 제어 기능을 악용하여 임의 인증을 수행 할 수 있으며, 결제 비밀번호 이외의 어떠한 정보를 요구하지 않음

- 또한, 역공학을 통해 인증 메시지 생성 알고리즘의 생성규칙을 파악이 가능 할 경우, 타 기기에서도 발신번호 조작을 통한 인증 위협이 존재

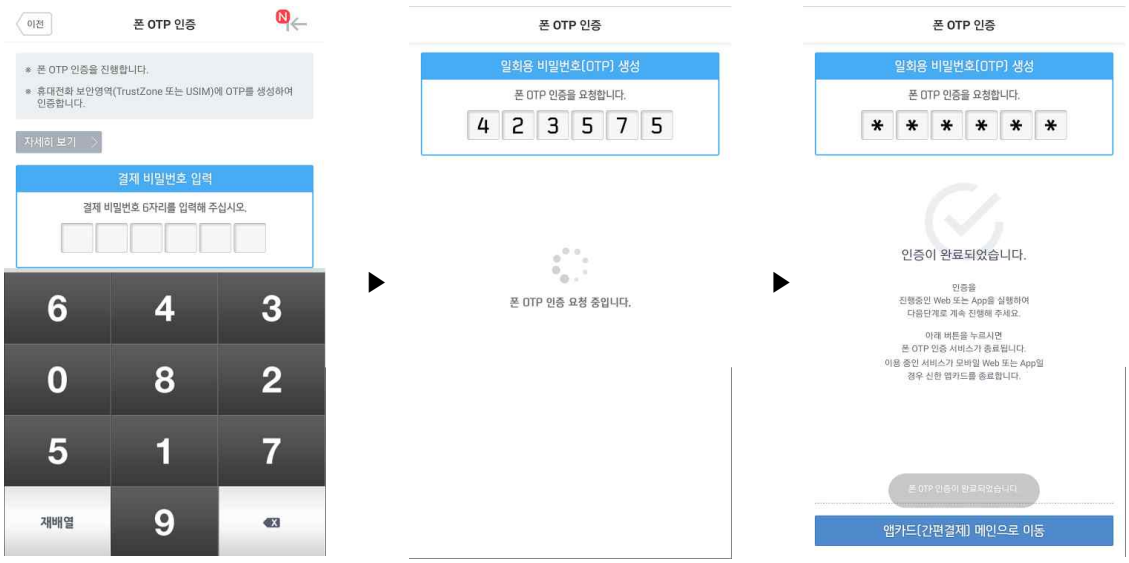
□ 폰OTP 인증

o 프로세스가 일반영역(Normal World)과 보안영역(Secure World)으로 구분된 스마트폰을 이용하여, 보안영역에서 일회용비밀번호(OTP)를 생성하여 인증하는 서비스임

※ 현재는 TrustZone을 지원하는 안드로이드 기반 스마트폰에서만 기능 지원

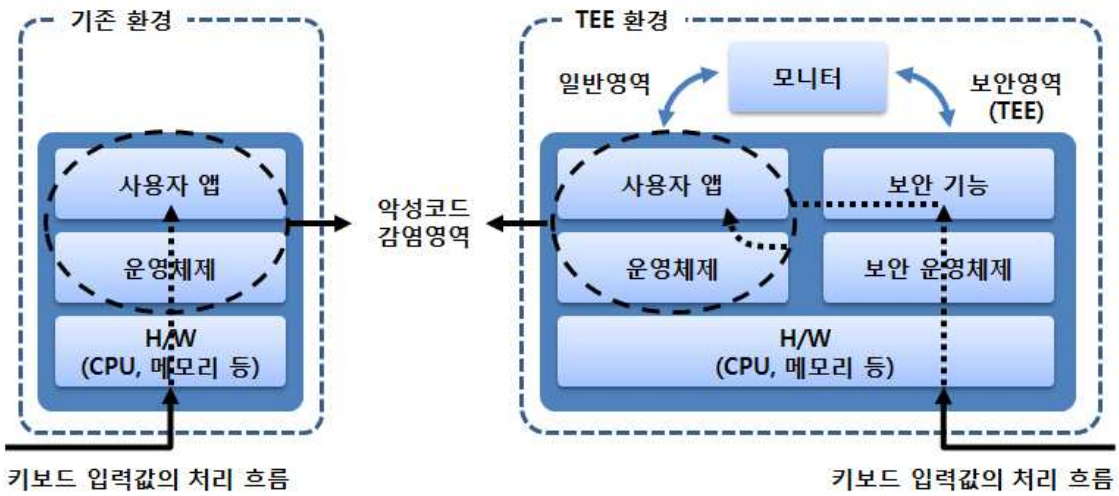
- **(편의성)** 이용자는 보안영역의 이용여부를 인지하지 못하므로 절차가 추가되거나 번거로움이 발생되지 않음
- **(보안성)** 일회용비밀번호 값을 생성되는 위치가 일반영역이 아니므로 상대적으로 높은 보안성을 제공

< 폰OTP 인증 절차 >



o **(보안영역)** H/W적으로 분리되고 신뢰된 실행환경(TEE)[4]에서 애플리케이션을 구동하므로 일반영역에서 접근이 불가함

< 기존 환경과 TEE환경 구조 >



4) TEE(Trusted Execution Environment)

o **(위험성)** 취약점, 중간자공격 등을 통한 데이터 유출 위험성이 존재함

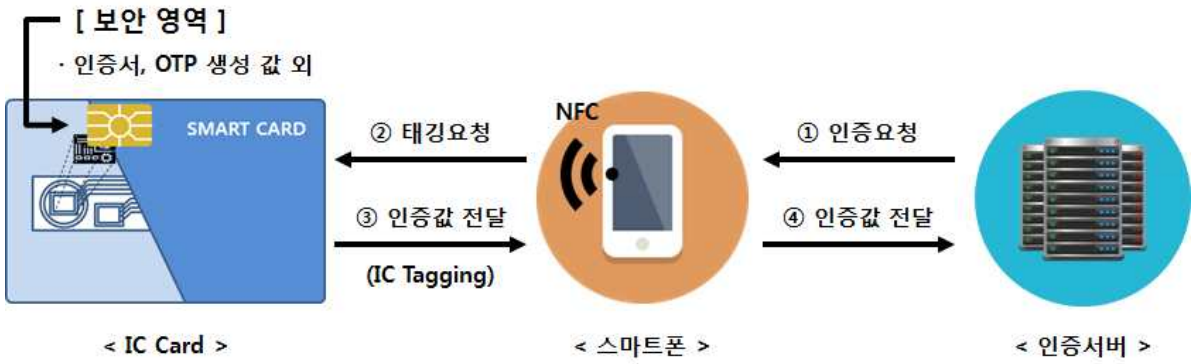
- **(취약점)** 펌웨어(Firmware), 커널(Kernel) 등의 취약점을 통해 보안영역의 데이터에 접근하는 등의 악용사례가 지속적으로 보고[5)]
- **(중간자공격)** 생성된 인증 값은 인증서버로 전달하기 위해 일반영역을 거쳐 인증서버와 암호화 통신을 하므로, 취약점 혹은 키 값이 노출될 경우 인증 값 탈취 가능

□ IC 태깅 인증

o IC카드에 등록된 사용자 식별정보나 탑재된 인증모듈(인증서, OTP 등)로부터 생성된 인증정보를 NFC 방식을 통해 모바일 기기로 전송하여 인증하는 방식임

- **(편의성)** 이용자는 보안영역을 이용하고 있다는 것을 인지하지 못하므로 절차가 추가되거나 번거로움이 발생되지 않음
- **(보안성)** 실물 IC카드를 추가로 소지해야만 인증이 가능

< IC 태깅 인증 절차 >



o **(위험성)** IC칩 복제, 메모리덤프, 중간자공격 등을 통한 데이터 유출 위험성이 존재함

- **(IC칩 복제)** 특수 복제 장비를 이용하여 IC칩을 복제하여 인증 수행

※ 단, 다른 단말기에서 이용하기 위해서 앱 설치 과정을 우회해야 함

5) 금융보안원, "최신 안드로이드 트러스트존(TrustZone) 취약점 상세 분석(2015.10.21.)" 참조

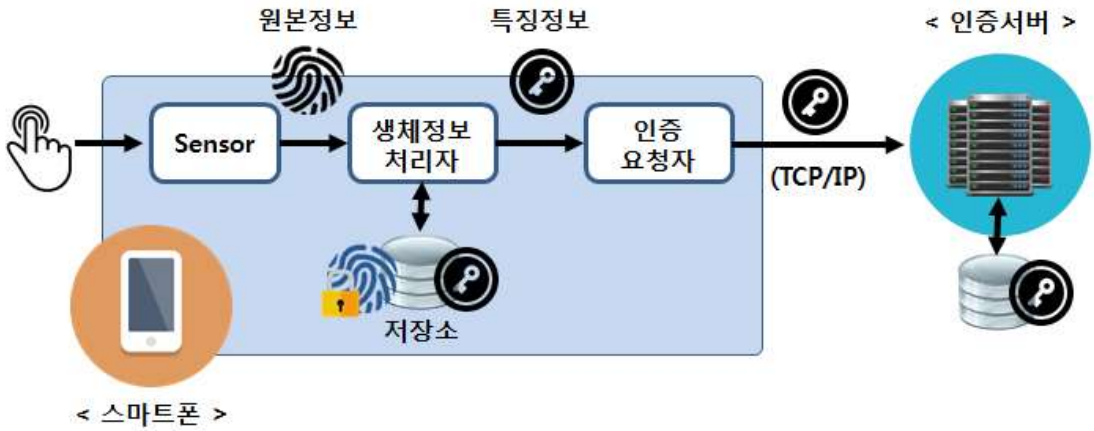
- **(메모리덤프)** 인증서버로 전달되기 전 스마트폰의 메모리상에 저장된 인증 값을 외부로 전달하여 인증하는데 이용
- **(중간자공격)** 인증서버로 태깅 값을 전달할 때 통신구간의 취약점 혹은 노출된 암호화 통신 키 값으로 전달되는 인증 값 탈취

□ 바이오 인증

o 지문, 홍채, 정맥, 목소리, 얼굴 등 이용자의 생체 혹은 행위 정보를 이용하기 위한 인증 방식임

- **(편의성)** 키 입력 절차 생략
- **(보안성)** 이용자 본인만이 인증이 가능한 방식으로 복제가 쉽지 않으며, 바이오 정보가 단말기 내부의 보안영역에 저장되어 유출위험이 낮음

< 지문을 활용한 바이오 인증 절차 >



o **(위험성)** 스마트폰에 내장된 바이오 인증 모듈은 보급형 장치로써, 위·변조 탐지가 어렵고, 재전송(Replay) 공격 등의 위험성이 존재함

- **(위·변조)** 실리콘 지문, 고해상도 사진 출력 등을 이용한 인증 우회로 인한 사고 혹은 악용 사례가 지속적으로 보고[6)]
- **(재전송 공격)** 인증에 성공된 네트워크 정보를 재전송하여 인증 우회

6) 금융보안원, "바이오정보 사고사례 및 대응방안 조사(2016.3.7.)" 참조

3. 비교 분석

o 서비스 이용 제약(단말기, 운영체제, 기능 등)에 의해 범용성, 보안성 등의 차별점이 존재함

< 대체 본인인증 서비스 비교 >

구 분	ARS/SMS 인증	휴대폰 인증	폰OTP 인증	IC 태깅 인증	바이오 인증
제공 여부	제공 중	제공 중	제공 중	제공 중	제공예정
이용 조건	없음	스마트폰	보안영역을 지원하는 프로세스	NFC 기능을 지원하는 스마트폰주1)	인증 모듈 (지문/홍채 인식 등)
기입 정보	(ARS) 인증번호 (SMS) 성명, 생년월일, 전화번호주2)	결제비밀번호	결제비밀번호	IC 카드 터치	바이오정보 (지문, 홍채, 목소리 등)주3
인증 주체	이동통신사	이동통신사	금융회사, 이동통신사주4)	금융회사	금융회사 (단말기)
인증 정보 생성 주체	이동통신사	단말기	단말기 (보안영역)	IC카드 (+단말기)주5)	단말기 (보안영역)
위험성	착신전환, 악성코드, 통신장비 조작	원격 제어, 역공학	취약점, 중간자공격	IC칩 복제, 메모리덤프, 중간자공격	위·변조, 재전송 공격
이슈	SMS 인증은 위험성을 고려하여 단독으로 사용되지 않음	아이폰 이용 시 문자를 직접 전송해야 함	관련 기능 모듈(보안영역, NFC, 바이오인증 등)을 요구하므로, 비교적 최신의 단말기 사용 조건이 필요함		

주1) 아이폰의 NFC 기능을 애플페이(Apple Pay)에서만 이용 가능하므로, 이용 제약 발생
주2) 경우에 따라 입력정보가 조금씩 상이함
주3) 서비스 출시 전으로 정확한 확인 불가능
주4) USIM 기반일 경우(현재 기능 미지원)
주5) 인증 정보는 IC카드에서 생성되나 단말기가 없으면 인증 정보를 읽을 수 없음

4. 시사점

o 공인인증서 의무 사용이 폐지된 후 공인인증서를 이용한 본인인증을 대체하기 위해 휴대폰 기반 본인인증 서비스가 등장하고 있으며, 인증 정보를 안전하게 생성·전달하기 위해 다양한 보안 기술이 적용되고 있음

o 단말기, 추가 인증수단(IC카드)을 통해 인증 정보를 생성하는 것이 상대적으로 안전하지만, 생성되는 위치(일반영역, 보안영역)에 따라 보안성, 위험의 정도가 달라짐

o 지속적으로 발생되는 위협으로부터 이용자를 보호하기 위해서는 사전에 등록된 단말기 기반 인증 이외에도 FDS[7], 거래연동 인증, TUI 등의 추가적인 보안 방안을 적용을 고려해야 함

- **(FDS)** 다양한 수집 데이터를 활용하여 부정인증 시도 여부를 판별하고, 유사한 위협에 대해서는 신속한 정보 공유 등의 대응 방안 고려
- **(거래연동 인증)** 인증 값 생성 시 거래 정보와 연동하여 본인의 거래 내역을 확인하여 보안 강화
- **(Trusted UI, TUI)** 일반영역의 입·출력 값은 캡쳐, 키로깅 등의 위험에 노출되므로 보안영역에 구현하여 입·출력 값 보호 필요

7) FDS(Fraud Detect System)

[참고] 카드사별 본인인증 서비스 제공 내역 및 테스트 환경

□ 테스트 환경

o 인증을 위해서 특정 기능을 제공하는 모바일 기기와 운영체제, 카드사에서 제공하는 앱 설치가 필요하며, 바이오 인증은 현재 제공 중이지 않아 일반적인 내용을 바탕으로 작성함

o **(모바일)** iPhone 6, Galaxy Note5

구분	iPhone6	Galaxy Note5
운영체제	iOS 9	Android 6
NFC 지원	△*	○
지문인식 지원	○	○
TEE 지원	○	○

* NFC 기능은 애플페이에서만 이용 가능함

□ 카드사별 본인인증 서비스

o 현재(2016.4월 기준) 카드사별 본인인증 서비스를 지원하는 내용으로, 접근 과정 등에 따라 다소 상이 할 수 있음

구분	제공 중인 인증서비스
KB국민카드	공인인증서, ARS인증(아웃바운드), 휴대폰인증(앱안심인증)
NH농협카드	공인인증서, SMS인증
롯데카드	공인인증서, SMS인증
삼성카드	공인인증서, ARS인증(아웃바운드), SMS인증
신한카드	공인인증서, ARS인증(인바운드), 폰OTP, IC태깅
씨티카드	공인인증서, ARS인증(아웃바운드)
하나카드	공인인증서, SMS+ARS인증(아웃바운드)
현대카드	공인인증서, ARS인증(인바운드)
비씨카드	공인인증서, ARS인증(아웃바운드)

구분	제공 중인 인증서비스
IBK기업은행카드	공인인증서, ARS인증(아웃바운드)
KDB카드	공인인증서, ARS인증(아웃바운드)
SC은행리워드카드	공인인증서, ARS인증(아웃바운드)
광주카드	공인인증서, ARS인증(아웃바운드)
수협카드	공인인증서, ARS인증(아웃바운드)
신협체크카드	공인인증서, ARS인증(아웃바운드)
우리카드	공인인증서, ARS인증(아웃바운드)
우체국카드	공인인증서, ARS인증(아웃바운드)
전북카드	공인인증서, ARS인증(아웃바운드)
제주카드	공인인증서, ARS인증(아웃바운드)
현대증권체크카드	공인인증서, ARS인증(아웃바운드)