금보원 2014-06

스마트폰 전자금융서비스 보안 가이드

2014. 7

금융보안연구원
Financial Security Agency

본 스마트폰 전자금융서비스 보안 가이드는 새로운 IT기술과 전자적 장치를 활용한 전자금융거래의 안전성 확보를 위해 금융회사가 참고할 수 있는 보안 가이드입니다.

본 가이드는 스마트폰 전자금융서비스 보안에 대한 최소한의 보안 방안에 대하여 제시하며, 안전한 전자금융서비스 환경을 구현하고 제공하는데 활용할 수 있습니다.

개 정 이 력

버전	날짜	변경내용	책임자
Ver 1.0	2014. 7. 8	• 최초작성	성 재 모

머 리 말

최근 스마트폰을 이용한 다양한 전자금융서비스의 발전과 함께 금융거래정보 탈취 및 변조 등 관련 보안위협이 증가하면서 안전한 보안방안과 대응 기술에 대한 연구가 시급히 필요한 상황입니다. 또한 향후 모바일 전자금융거래의 급속한 확산이 예상됨에 따라 보안 기술의 개발을 위한 가이드가 필요한 시점이기도 합니다.

이번『스마트폰 전자금융서비스 보안 가이드』는 2010년 12월 발간된『금융부문 스마트폰 보안 가이드』를 토대로 그 동안 획기적으로 진행된 새로운 IT기술과 전자적 장치 활용을 포함하여 전자금융거래의 안전성 확보를 위해 금융회사가 참고할 수 있는 보안기술 가이드입니다.

본 가이드에서는 금융 앱의 설계 및 개발, 이용자에게 안전한 서비스 제공, 시스템 및 보안 관리의 3단계로 구분하여 각 단계별로 보안위협에 대응하는 스마트폰 전자금융서비스를 위한 최소한의 보안 기술 방안을 포함하고 있습니다.

금융보안연구원은 이러한 결과물을 바탕으로 금융회사에 대한 안전한 스마트폰 전자금융서비스 제공 및 보안 기술 발전을 위해 지속적으로 분석・연구하도록 하겠습니다. 본 가이드가 안전한 전자금융서비스 환경을 구현하고 제공하는데 많은 도움이 되길 바라며 본 가이드 작업에 수고해 주신 여러분들께 감사의 말씀을 전합니다.

2014년 7월

금융보안연구원

원장 김 영 린

< 목 차 >

제1장 개 요 ····· 3

제1절 배경 및 목적 ····· 3
제2절 적용대상 및 범위 ····· 4
제3절 구성 ····· 4
제4절 용어 정의 ····· 4

제2장 스마트폰 전자금융서비스 보안위협 ····· 9

제1절 스마트폰 전자금융서비스 구성 ····· 9
제2절 스마트폰 전자금융서비스 보안위협 ····· 11
제3절 스마트폰 전자금융서비스 보안위협 시나리오 ····· 15

제3장 스마트폰 전자금융서비스 보안 ····· 23

제1절 스마트폰 전자금융서비스 보안 기본원칙 ····· 23
제2절 스마트폰 전자금융서비스 보안방안 ····· 26
1. 안전한 앱 구현 ····· 26
2. 보안 기능 적용 ····· 28
3. 앱 보안성 확인 ····· 30
4. 안전한 앱 배포 ····· 31
5. 앱 업데이트 관리 ····· 32
6. 설치·실행 환경 관리 ····· 33
7. 앱 무결성 검증 ····· 34
8. 이용자 확인 강화 ····· 36
9. 안전한 통신 ····· 37
10. 이용자 교육 ····· 39
11. 시스템 보안 ····· 41
12. 보안 관리 ····· 42

[참고문헌] ····· 43

[부록 1] 스마트폰 전자금융서비스 보안 고려사항 ····· 49

제1절 프로그램 개발 시 고려사항 ····· 49
제2절 스마트폰 전자금융서비스 안전대책 점검방법 ····· 53
제3절 전송정보 암호화 ····· 56
제4절 앱 기반 Push 서비스 구성 및 보안 고려사항 ····· 58

[부록 2] 안전한 스마트폰 전자금융서비스 배포 방안 ····· 63

[부록 3] 스마트폰 전자금융서비스 이용자 유의사항 ····· 67

<그림 목차>

<그림 1> 스마트폰 전자금융서비스 구성 ····· 9
<그림 2> 스마트폰 전자금융서비스 관련 보안위협 ····· 15
<그림 3> 스마트폰 전자금융서비스 보안(3단계) ····· 23
<그림 4> 앱 기반 Push 서비스의 일반적 구조 ····· 58
<그림 5> 앱 기반 Push 서비스의 보안 위협 ····· 59
<그림 6> '알 수 없는 출처' 기능 예 ····· 63
<그림 7> 루팅, 탈옥 예 ····· 67
<그림 8> 금융 앱 설치 안내 화면 예 ····· 68
<그림 9> SMS 링크(URL) 예 ····· 69
<그림 10> 안드로이드 운영체제 보안설정 예 ····· 70
<그림 11> 보안승급 등 금융회사 사칭 예 ····· 71
<그림 12> 금융정보 저장 예 ····· 72
<그림 13> 공인인증서 재발급 안내 예 ····· 75
<그림 14> 스마트폰 운영체제 업데이트 안내 예(iTunes 사용) ····· 77
<그림 15> 스마트폰 운영체제 업데이트 안내 예(스마트폰에서 실행) · 77
<그림 16> 악성코드 검사 예 ····· 78
<그림 17> 악성코드 검사 전용 프로그램 업데이트 예 ····· 78

<표 목차>

[표 1] 스마트폰 전자금융서비스 설계·개발단계 보안위협 ····· 11
[표 2] 스마트폰 전자금융서비스 설치·이용단계 보안위협 ····· 13
[표 3] 스마트폰 전자금융서비스 시스템·관리 단계 보안위협 ····· 14
[표 4] 권고 대칭키 암호 알고리즘 및 키 길이 ····· 56
[표 5] 권고 공개키 암호 알고리즘 및 키 길이 ····· 56
[표 6] 보안 강도별 암호알고리즘 ····· 57
[표 7] 앱 기반 Push 서비스 구분 ····· 58

제1장 개 요

제1장 개 요

제1절 배경 및 목적

최근 스마트폰 이용자의 증가와 다양한 금융 앱의 출시로 스마트폰을 기반으로 한 전자금융서비스를 이용하는 고객이 증가하고 있다.

한편 스마트폰 앱 위조 혹은 악성 앱 설치를 통해 금융거래와 관련된 중요정보를 탈취하거나, 금융거래 정보의 변조를 통해 금전적 이득을 취하는 등 보안위협도 지속적으로 증가하고 있다. 따라서, 스마트폰에서 전자금융서비스를 제공하는 응용프로그램으로써 “앱”은 설계·개발 과정에서부터 설치·이용 과정까지 안전한 관리가 요구된다.

이에 본 가이드는 스마트폰 전자금융서비스 앱의 설계·개발 과정부터 설치·이용 및 시스템·관리 단계를 포함하여 단계별 보안 가이드를 제공함으로써 금융회사가 이용자에게 안전한 서비스를 제공하는데 도움을 주고자 한다.

제2절 적용대상 및 범위

o 적용대상 : 스마트폰 기반 전자금융서비스를 제공하는 금융회사 및 전자금융업자

o 범　　위 : 스마트폰에서 전자금융거래를 제공하는 앱 기반 전자금융서비스

제3절 구성

본 가이드는 1장에서 목적, 적용대상, 범위 등을 정의하고, 2장에서 스마트폰 전자금융서비스 구성 및 보안위협을 살펴보고, 3장에서 기본원칙과 상세 보안방안을 기술한다.

제4절 용어 정의

본 보안 가이드에서 사용되는 용어 정의는 다음과 같다.

- 전자금융거래 : 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래 (전자금융거래법 제2조 1항)
- 스마트폰 : 휴대폰에 컴퓨터 지원기능을 추가한 지능형 휴대폰으로, 휴대폰 기능에 충실하면서 수기방식의 입력장치와 터치스크린 등 보다 사용에 편리한 인터페이스를 갖추고 있음. 다양한 기능의 수용을 위하여 표준화된 또는 전용 운영체제(OS)를 갖추기도 함

- 앱(App) : 스마트폰 등 모바일기기 운영체제(OS)에서 실행될 수 있도록 개발된 애플리케이션(Application)
- 앱 스토어(App Store) : 개발자들이 개발한 어플리케이션을 등록하고 사고 팔 수 있는 온라인장터(Market Place)
- 난독화 : 난독화는 작성된 코드를 읽기 어렵게 만들어 역공학 공격에 대비할 수 있는 기술로서 암호화, 안티 디버깅, 가상화 등의 기법을 활용
- 루팅(Rooting), 탈옥(Jail Break) : 루팅(Rooting) - Google사의 Android 운영체제 기반의 스마트폰 보안기능을 해제하여 유료 프로그램을 무료로 사용하거나, 개인의 취향에 맞도록 기능 및 성능 등을 개선하는 행위

  탈옥 - Apple사의 iOS 운영체제 기반의 스마트폰 보안기능을 해제하여 유료 프로그램을 무료로 사용하거나, 개인의 취향에 맞도록 기능 및 성능 등을 개선하는 행위
- 배포 인증서 : 개발된 앱 프로그램을 배포하기 위해 배포처에서 요구하는 인증서
- 무결성 : 프로그램, 데이터 등을 인가되지 않은 방법으로 변경할 수 없도록 보호하는 성질
- 피싱(Phishing) : 프라이버시(Privacy)와 낚시(Fishing)의 합성어로써, 이메일, 인터넷, 휴대폰, 메신저 등을 이용하여 기관 홈페이지나 인물로 사칭하여 개인정보를 불법적으로 획득하는 행위
- 스미싱(Smishing) : 문자메시지와 피싱의 합성어로 문자메시지 내 악성코드 링크를 클릭하는 경우 악성코드가 스마트폰에 설치

- 파밍(Pharming) : 금융회사 등의 정상적인 홈페이지 주소로 접속하여도 피싱(가짜)사이트로 접속하도록 유도

- 큐싱(Qshing) : QR코드(Quick Response Code)와 피싱(Fishing)의 합성어로 QR코드를 스마트폰으로 스캔 시 공격자에 의해 의도된 악성 URL로 접속되어 악성 앱을 다운받아 설치도록 유도하는 수법

- API(Application Program Interface) : 프로그램 또는 애플리케이션이 운영 체제에 어떤 처리를 위해서 호출할 수 있는 서브루틴 또는 함수의 집합

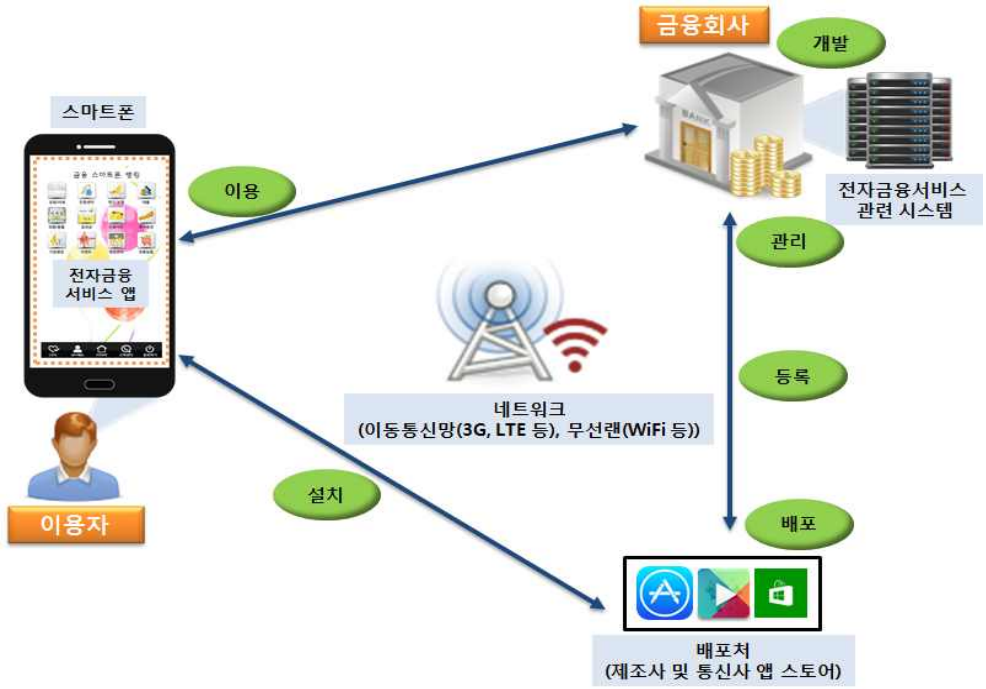
제2장 스마트폰 전자금융서비스 보안위협

제2장 스마트폰 전자금융서비스 보안위협

제1절 스마트폰 전자금융서비스 구성

스마트폰 전자금융서비스란 금융회사가 스마트폰을 통하여 금융상품 및 서비스를 제공하고, 이용자가 금융회사의 종사자와 직접 대면하거나 의사소통을 하지 않고 스마트폰 전자금융서비스 앱을 이용하여 자동화된 방식으로 이를 이용하는 거래 서비스를 말한다.

이러한 스마트폰 전자금융서비스는 별도의 단말기나 네트워크를 구성할 필요 없이 이용자가 소유하고 있는 스마트폰과 스마트폰에서 이용 가능한 네트워크(이동통신망, Wi-Fi 등)를 사용하여 이용된다. 스마트폰 전자금융서비스 이용을 위한 구성요소는 아래와 같다.



<그림 1> 스마트폰 전자금융서비스 구성

- 금융회사 : 스마트폰 전자금융서비스를 제공하기 위하여 스마트폰에서 설치·실행되는 전자금융서비스 앱 및 관련 시스템을 개발·관리한다.
- 스마트폰 : 이용자 개인의 모바일 기기로써, 하드웨어(H/W)와 운영체제(구글의 안드로이드, 애플의 iOS 등 응용프로그램들의 설치·실행을 관리)로 구성되며, 전자금융서비스를 이용하기 위해서는 전자금융서비스 앱이 설치 및 실행된다.
- 네트워크 : 스마트폰 특성상 이동통신망(3G, LTE 등)과 무선랜(Wi-Fi 등)을 이용하여 통신한다.
- 배포처 : 스마트폰에 탑재할 수 있는 애플리케이션을 판매하는 곳으로 제조사 앱 스토어(애플의 앱스토어, 구글의 플레이스토어 등), 통신사 앱 스토어(SKT의 티스토어, KT의 올레마켓, LG U+ 스토어 등) 등이 있다. 금융사는 스마트폰 전자금융서비스 앱을 이곳에 등록하고, 이용자는 이곳에서 전자금융서비스 앱을 다운로드 받을 수 있다.

제2절 스마트폰 전자금융서비스 보안위협

안전한 스마트폰 전자금융서비스의 제공을 위해 구성요소에 따라 주요 보안위협을 사전에 파악해야 한다. 보안위협은 전자금융서비스 제공 단계와 더불어 개발 단계부터 파악하여야 하며, 시스템 보안 및 서비스 관리 등 지속적인 노력을 통해 이용자에게 안전한 전자금융서비스를 제공하여야 한다.

이에 본 가이드에서는 스마트폰 전자금융서비스 보안위협을 설계·개발, 설치·이용, 시스템·관리의 3단계로 구분하고, 구성요소에 따라 보안 위협을 분류한다.

1. 설계·개발 단계 보안위협

설계·개발 단계의 보안위협은 스마트폰 전자금융서비스 앱의 개발과 배포 과정으로 구분된다. 앱 개발 시 위협은 소스코드 보안 약점, 전자금융서비스 앱 보안기능 약화 시 위협을 포함하며, 배포 시 위협은 검증되지 않은 앱을 배포하였을 때 보안위협이 있을 수 있다. 설계·개발 단계의 구성요소에 따른 위협의 분류는 다음과 같다.

구성요소	보안위협
앱 (설계·개발 시)	• 프로그램 입력값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안약점 • 검증되지 않은 외부 입력값이 시스템 자원의 접근경로 또는 자원 제어에 사용되어 공격자가 입력값을 조작해 공격할 수 있는 보안약점 • 외부 입력값의 유효성(지정된 길이 초과, 악성코드 포함 등) 검증하지 않아 발생할 수 있는 보안 취약점

	• 멀티프로세스 상에서 자원을 검사하는 시점과 사용하는 시점이 달라서 발생하는 보안약점 • 종료조건 없는 제어문 사용으로 반복문 또는 재귀함수가 무한히 반복되어 발생할 수 있는 보안약점 • 중요자원(프로그램 설정, 민감한 사용자 데이터 등)에 대한 적절한 접근권한을 부여하지 않아, 인가되지 않은 사용자 등에 의해 중요정보의 노출·수정 • 중요정보의 기밀성을 보장할 수 없는 취약한 암호화 알고리즘의 사용으로 인한 정보 노출 • 중요정보 전송 시 암호화하지 않거나 안전한 통신채널을 이용하지 않아 정보가 노출 • 모바일 애플리케이션 소스코드 분석(리버스 엔지니어링)을 통한 취약점 분석 • 원격으로부터 소스코드 또는 실행파일을 무결성 검사 없이 다운로드 받고 이를 실행하는 경우, 공격자가 악의적인 코드를 실행할 수 있는 보안약점 • 개발자가 생성한 오류 메시지에 시스템 내부구조 등이 포함되어 민감한 정보가 노출될 수 있는 보안약점 • 예외에 대한 부적절한 처리로 인해 의도하지 않은 상황이 발생될 수 있는 보안약점 • 취약하다고 알려진 함수를 사용함으로써 예기치 않은 보안위협에 노출될 수 있는 보안약점 • 파일의 확장자 등 파일 형식에 대한 검증없이 업로드를 허용하여 발생할 수 있는 보안약점
앱 및 배포처 (등록·배포 시)	• 악의적 개발자에 의한 악성 프로그램 배포 • 보안 메커니즘을 우회한 악성프로그램 등록 • 앱의 개인정보 전송 여부 등 기능에 대한 완전한 인식 부족으로 데이터 유출 가능성 존재 • 문자 메시지, 이메일, 일반 홈페이지 등을 이용하여 악성 애플리케이션(가짜 앱 등) 유포 • 공유기 DNS 서버 변경 및 큐싱(Qshising)을 통한 악성 앱 유포

[표 1] 스마트폰 전자금융서비스 설계·개발단계 보안위협

2. 설치·이용 단계 보안위협

설치·이용 단계의 보안위협은 스마트폰 전자금융서비스 앱 이용 시 구성요소인 스마트폰(단말/플랫폼), 전자금융서비스 앱(애플리케이션), 이동통신망·무선 네트워크(네트워크)에 따라 분류하면 다음과 같다.

구성요소	보안위협
스마트폰 (단말/플랫폼)	• 악성코드를 통한 단말기 녹음, 녹화, 화면캡처, 메모 기능을 통해 생성·저장된 정보 유출 • 악성코드를 통한 지속적인 통화연결 및 데이터 전송 요청으로 배터리 소진 등 단말기 서비스 거부 공격 • 악성프로그램 감염을 통한 신용카드 정보, 뱅킹 인증 정보 등을 탈취 및 변조 • 키로거(key logger) 감염에 의한 이용자 입력정보 탈취 • 단말기에서 제공하는 테더링 및 USB 기능을 사용하여 악성코드 전파 및 서버 보안 정책 우회 등 공격 경로로 활용 • 플랫폼 변조를 통한 펌웨어 변조, 관리자 권한 탈취, 파일 정보 접근 (응용프로그램 파일, 공인인증서 파일 등 추출 가능) • 어깨 너머로 모바일 장치 화면의 민감한 데이터에 노출
전자금융서비스 앱 (애플리케이션)	• 비인가 애플리케이션 설치에 따른 정보유출 • 위·변조 앱의 설치에 따른 보안카드나 이체 비밀번호 등 입력하는 중요정보의 유출 • 위·변조 앱의 설치에 따른 금융관련 중요정보가 화면에 출력될 때 화면캡쳐 및 원격제어를 통한 출력정보의 유출 • 악의적인 사이트, 문자 메시지, 이메일 등을 이용하여 악성 애플리케이션(가짜 앱 등) 설치 유도 및 정보 수집 • 악성코드가 삽입된 애플리케이션을 통한 인증정보 탈취
이동통신망·무선 네트워크 (네트워크)	• 단말기-내부시스템에 대한 중간자(Main-in-the-Middle) 공격을 통한 사용자 권한 획득 • 단말기와 내부 시스템 간에 맺혀진 세션 탈취 • 네트워크로 전송되는 데이터 패킷 도청 • 비인가 AP, 블루투스 및 Wi-Fi Direct 취약점을 이용한 정보유출

[표 2] 스마트폰 전자금융서비스 설치·이용단계 보안위협

3. 시스템·관리 단계 보안위협

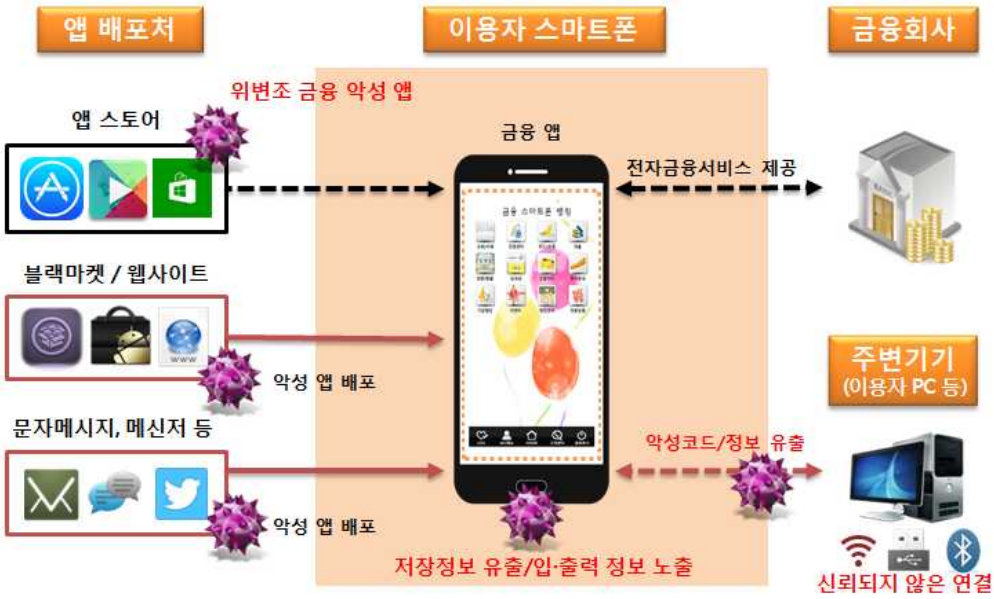
시스템·관리 단계의 보안위협은 스마트폰 전자금융서비스 앱의 구성요소인 전자금융서비스 관련 시스템(내부 시스템)과 서비스 보안관리(보안관리)에서 발생할 수 있는 보안 위협으로 구분된다.

구성요소	보안위협
전자금융서비스 관련 시스템 (내부 시스템)	• 좀비 스마트폰 등을 이용한 내부 서버 대상의 서비스 거부 공격 • 불필요한 데이터 수집으로 인한 데이터 오용 및 유출 • 전자금융거래에 대한 약한 감사 적용으로 거래의 감사 추적이 불가능
서비스 보안관리 (보안관리)	• 문자 메시지, 이메일 등을 이용하여 악성 애플리케이션(가짜 앱 등) 설치 유도, 정보 수집 • 단말기 분실·도난 시 기기 내부에 저장된 중요정보의 유출

[표 3] 스마트폰 전자금융서비스 시스템·관리 단계 보안위협

제3절 스마트폰 전자금융서비스 보안위협 시나리오

스마트폰 전자금융서비스는 앱을 기반으로 서비스가 제공되기 때문에 앱을 배포하는 경로로 활용될 수 있는 앱 스토어, 블랙마켓, 웹사이트, 문자메시지, 메신저 등을 이용한 공격과 단말기 자체 특성에 기인하여 PC 등 주변기기와 연동 시 발생할 수 있는 취약점을 이용한 공격 등이 이루어질 수 있다.<그림 2>



<그림 2> 스마트폰 전자금융서비스 관련 보안위협

이러한 공격을 통해 스마트폰 전자금융거래 시 거래정보의 입력, 출력, 전송, 저장 과정에서 '중요정보 유출'의 보안위협이 발생할 수 있다.

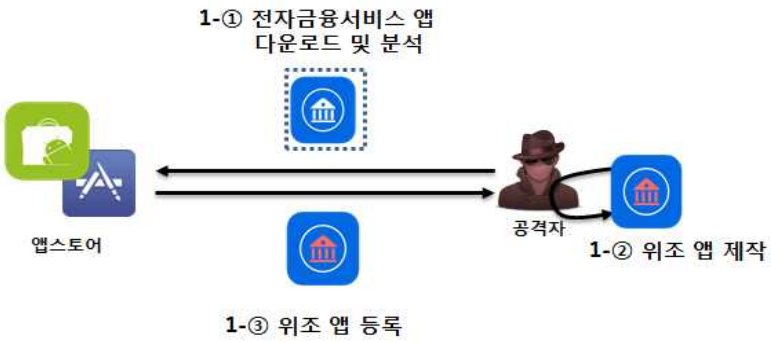
- 입력 : 보안카드나 이체 비밀번호 등 금융 앱이 실행된 상태에서 입력하는 중요정보의 유출
- 출력 : 금융 관련 주요정보가 화면에 출력 될 때 화면캡처 및 원격제어를 통한 중요정보의 유출

- 저장 : 악성코드 감염이나 단말기 분실 등의 상황에서 기기 내부에 저장된 중요정보의 유출
- 전송 : 유·무선 통신 기능 이용 시 전송 될 수 있는 중요정보의 유출

다음은 스마트폰 전자금융서비스 이용 시 정보 유출과 관련하여 발생 가능한 보안위협 시나리오로써, 공격자는 스미싱을 통해 이용자 스마트폰에 위조 앱을 설치하거나 악성코드에 감염된 PC를 통해 악성 앱을 설치하여 공격을 수행할 수 있다.

- 스미싱을 통한 위조 앱 설치

[1 단계] 스마트폰 전자금융서비스 앱 취약점 분석 및 앱 위조



① (공격자) 검증된 앱 스토어에서 전자금융서비스 앱을 다운로드 받아 역공학 분석(reverse engineering) 등을 통해 앱의 API, 함수 등 동작원리, 주요 기능을 분석한다.

② (공격자) 분석을 통해 얻은 정보를 바탕으로 전자금융서비스 앱을 가장한 악의적인 위조 앱(이하 위조 앱)을 제작한다.

③ (공격자) 위조 앱을 앱 스토어에 등록한다.

※ 공식 앱 스토어가 아닌 블랙마켓 등에서 앱을 다운로드 할 경우, 위조 앱(악성 앱)에 감염될 위험이 더 큼

[2 단계] 스미싱을 통한 위조 앱 설치

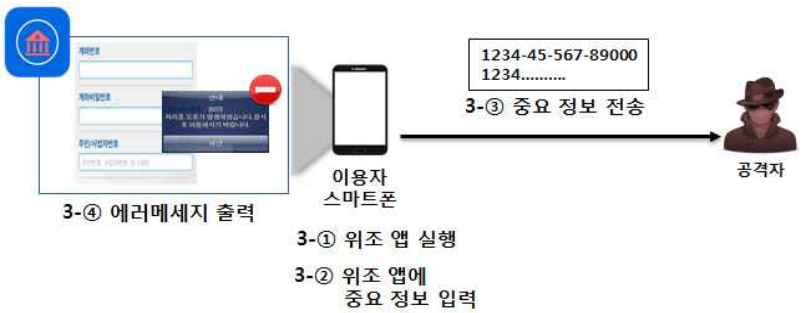
① (공격자) 위조 앱을 다운로드 받도록 앱 스토어에 연결하는 URL이 포함된 문자메시지를 불특정 다수에게 발신한다.

※ 문자 메시지 내용 예 : 전자금융서비스 앱 업데이트 공지, 신규 서비스 공지, 보안 프로그램 설치 권고 등

② (이용자) 문자메시지의 URL을 누르면 위조 앱이 다운로드 후 설치된다.

※ 안드로이드 운영체제를 탑재한 스마트폰의 경우, 악성 앱 설치 시 '알 수 없는 출처(소스)' 설정이 체크되어야 앱 설치 가능

[3 단계] 위조앱을 통한 이용자 정보 유출



① (이용자) 스마트폰 전자금융서비스를 이용하기 위해 위조 앱을 실행한다.

② (이용자) 서비스 이용을 위해 위조 앱에 개인정보 또는 금융거래 정보를 입력한다.

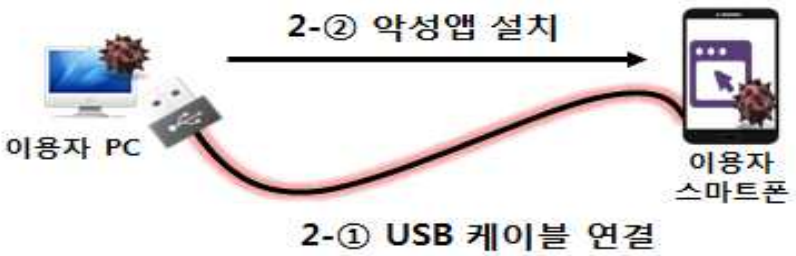
③ (공격자) 이용자가 입력한 정보는 이용자도 모르게 위조 앱을 통해 공격자에게 전송된다.
④ (공격자) 에러 메시지 등을 출력하여 공격자가 이용자의 중요 정보를 취득한 사실을 이용자가 인지하지 못하도록 한다.
※ 에러 메시지 예 : 전자금융서비스 이체 에러 등

■ PC를 통한 악성코드 감염

[1 단계] 취약한 웹 서버를 통한 PC 감염

① (공격자) 취약한 웹 서버를 해킹하여 이용자 PC가 악성코드에 감염될 수 있도록 웹페이지를 변조한다.
② (공격자) 변조된 웹페이지에 접속하는 이용자 PC의 취약점을 통해 강제로 악성코드를 감염시킨다.

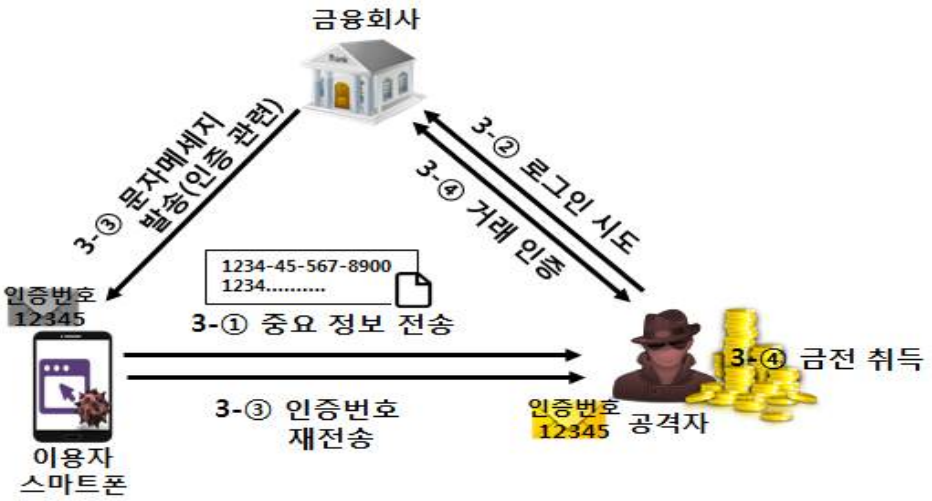
[2 단계] PC를 통한 악성 앱 설치



① (이용자) 스마트폰에 파일(음악, 영화, 문서 등)을 복사하기 위해 스마트폰과 PC를 USB케이블로 연결한다.

② (이용자) 스마트폰을 PC에 연결하면 악성코드에 감염된 PC에 의해, 스마트폰에 정보유출, 문자메시지 탈취 등 악성행위를 하는 앱(이하 악성 앱)이 이용자의 스마트폰에 강제로 설치된다.

[3 단계] 악성앱을 통한 이용자 정보 유출 및 금전 취득



① (공격자) 설치된 악성 앱은 스마트폰 내부에서 수집한 중요 정보(전자금융서비스 이용 시 필요한 금융정보)를 공격자에게 전송한다.

② (공격자) 공격자는 수집된 정보를 바탕으로 전자금융서비스에 로그인을 시도한다.

③ (공격자) 악성 앱은 거래 인증을 위해 발송된 문자메시지를 가로채 공격자에게 재전송하고, 이용자가 인지하지 못하도록 해당 문자메시지를 삭제한다.

④ (공격자) 문자메시지의 인증정보를 이용해 거래 인증 후 금전을 취득한다.

제3장 스마트폰 전자금융서비스 보안

제3장 스마트폰 전자금융서비스 보안

제1절 스마트폰 전자금융서비스 보안 기본원칙

본 가이드에서는 안전한 스마트폰 전자금융서비스를 제공하기 위해 이용자에게 안전한 서비스 제공 단계와 더불어 서비스 제공 이전에 금융앱의 설계 및 개발 보안 단계와 시스템 및 보안 관리 단계로 확장하여 3단계별로 구분하고 각 단계별 보안 원칙을 기술한다.

첫째, 앱 설계/개발 단계는 스마트폰 앱 설계 및 개발 시 보안 고려사항을 제시하고, 둘째, 설치/이용 단계에서는 이용자의 전자금융서비스 앱 설치·이용의 흐름에 따라 안전한 서비스 제공을 위한 보안 고려사항을 제시하며, 셋째, 시스템/관리 단계에서는 시스템 보안, 보안 관리에 대한 보안 고려사항을 제시한다.<그림 3>

<그림 3> 스마트폰 전자금융서비스 보안(3단계)

[앱 설계 및 개발 시 보안]

① **(안전한 앱 구현)** 안전한 전자금융서비스를 위하여 설계단계부터 보안을 고려하여 구현하여야 한다.

② **(보안 기능 적용)** 거래정보의 안전한 처리 등 스마트폰 전자금융서비스의 보안성 강화를 위한 기능을 고려하여 앱을 구현하여야 한다.

③ **(앱 보안성 확인)** 앱 배포 전 앱의 보안성과 안전성이 검증되어야 한다.

④ **(안전한 앱 배포)** 이용자에게 제공하는 앱은 공식 배포처를 이용하여 배포하여야 한다.

⑤ **(앱 업데이트 관리)** 안전한 서비스를 위해 앱 배포 후에도 보안성 확인 등 업데이트 관리가 되어야 한다.

[안전한 서비스 제공]

⑥ **(설치·실행환경 관리)** 운영체제의 임의 개조 및 악성코드 탐지 등 이용자의 앱 설치·실행 환경을 관리하여야 한다.

⑦ **(앱 무결성 검증)** 이용자에게 제공하는 앱의 위·변조여부 확인을 위하여 무결성을 검증하여야 한다.

⑧ **(이용자 확인 강화)** 스마트폰 전자금융서비스에서 이용자를 확인 및 강화 할 수 있는 절차와 방법을 마련하여야 한다.

⑨ **(안전한 통신)** 통신구간 암호화, 중요정보의 암호화, 거래전문 무결성 검증 등 안전한 통신을 위한 보안대책을 마련하여야 한다.

⑩ **(이용자 교육)** 전자금융서비스 이용자에게 안전한 서비스 이용을 위한 교육·홍보가 이루어져야 한다.

[시스템 및 보안 관리]

⑪ **(시스템 보안)** 스마트폰 전자금융서비스를 제공하기 위한 관련 시스템에 대한 보안이 이루어져야 한다.

⑫ **(보안 관리)** 안전한 서비스를 위해 접속정보·서비스 이용내역 제공, 분실·도난 시 대응절차 마련 등 지속적으로 관리되어야 한다.

제2절 스마트폰 전자금융서비스 보안방안

1. 안전한 앱 구현

스마트폰 전자금융서비스 앱은 소프트웨어 생명주기 모든 단계에서 보안성이 고려되어야 하며, 안전한 앱 개발을 위한 규칙을 준수 및 안전한 개발환경에서 앱을 구현하여야 한다.

- **(보안 요구사항 정의)** 앱 개발 시 기획 및 설계단계부터 금융보안 관련 법률·내외부 규정·기술 등 다양한 측면에서 보안성이 고려되어야 한다.

  ☞ 설계 시 보안고려 예시 : 전자금융서비스에 필요한 비즈니스 로직을 최대한 서버에서 처리 및 검증할 수 있도록 보안성을 고려하여 설계

- **(개발환경 구성)** 각종 위험에 대처 가능하도록 이용자 접근통제·침해대응·산출물 관리 등 개발 업무에 최적화된 개발 보안 환경을 구성하고 적절히 관리되어야 한다.

  ☞ 개발환경 구성(앱 빌드 및 서명용 PC 관리) 예시 : 개발자(금융회사) 서명용 인증서가 저장된 PC의 네트워크 격리, 담당자 지정 등

- **(테스트 데이터 이용)** 앱 개발 시 테스트에 사용되는 데이터는 개인정보 또는 금융거래정보를 포함해서는 안되며, 필요 시 테스트를 위한 가상의 데이터를 생성하여 이용하거나 테스트에 사용된 데이터는 모두 삭제하여야 한다.

- **(프로그램 작성)** 앱 개발 시 앱의 보안 취약점을 사전에 파악하고, 안전한 앱 개발을 위해 시큐어코딩* 등을 고려하여야 한다.

  * 시큐어코딩 : 소프트웨어 내에 존재하는 잠재적인 보안 취약점을 사전에 제거하여 외부 공격으로부터 안전한 소프트웨어를 개발하는 방법

  [참고] [부록 1] 제1절 프로그램 개발 시 고려사항

☐ Google사의 Android(Java)

- Android-JAVA 시큐어코딩 가이드
  - 출처 : 안전행정부(www.mopas.go.kr) > 정책자료 > 간행물 > 시큐어코딩 가이드(C, Java)
- Android Application Development Guidelines
  - 출처 : 미국 US-CERT(www.securecoding.cert.org) > Java > 50. Android(DRD)
- 『Androidアプリのセキュア設計・セキュアコーディングガイド』(Android 어플리케이션 보안 설계 및 코딩 가이드)
  - 출처 : 일본 스마트폰 보안 협회(www.jssec.org) > Report > 2014년 > 2014/05/01 JSSEC releases English version of Android Application Secure Design/Secure Coding Guidebook

☐ Apple사의 iOS(C/C++, Object-C)

- C 시큐어 코딩 가이드
  - 출처 : 안전행정부(www.mopas.go.kr) > 정책자료 > 간행물 > 시큐어코딩 가이드(C, Java)
- CERT C++ Secure Coding Standard
  - 출처 : 미국 US-CERT(www.securecoding.cert.org) > C++
- Secure Coding Guide
  - 출처 : 미국 애플(www.apple.com) > Resources > Developer Library > iOS7 또는 iOS8 > security > Secure Coding Guide

2. 보안 기능 적용

스마트폰 전자금융서비스 앱 이용 시 거래정보의 안전한 처리 등 스마트폰 전자금융서비스 보안성 강화를 위해서 요구되는 보안기능을 고려하여 앱을 구현하여야 한다.

- **(보안 기능 적용 및 강화)** 앱 개발 시 보안 위협 및 보안 취약점을 기반으로 보안기능(인증, 기밀성, 무결성, 암호화, 권한관리 등)을 적용 및 강화하여 개발하여야 한다.
- **(중요 기능의 고려)** 전자금융서비스 앱 개발 시 이용자 인증, 앱 무결성 검증, 거래전문 무결성 검증 등 보안성 강화를 위해 금융회사에서 정한 중요 기능이 고려*되어야 한다.

  * 아래 [개발 시 앱의 보안 기능 강화]를 참조하여 앱의 보안성을 강화할 수 있음

- **(앱 분석 방지)** 스마트폰 전자금융서비스에서 제공하는 중요기능이 악의적인 목적으로 변경되지 않도록 중요모듈 구현 시, 앱에 역 분석(Reverse Engineering) 방지 기술*을 적용하여야 한다.

  * 분석을 어렵게 하기 위해 중요 기능은 네이티브 라이브러리(C/C++ 계열) 등으로 구현하고, 시큐어 코딩, 바이너리(바이트 코드, 네이티브 코드 등)에 대한 난독화 등 적용

[개발 시 앱의 보안성 강화를 위한 중요 기능]

- **(앱 권한 관리)** 전자금융서비스 앱의 권한은 기능 동작에 필요한 최소 권한만 부여되게 개발되어야 한다.
- **(이용자 정보수집 최소화)** 개인정보 등 이용자 정보 수집 시 사전에 동의를 구하고, 최소한의 정보만을 수집하도록 하여야 한다.
- **(운영체제 임의 개조 탐지 및 이용제한)** 스마트폰 운영체제의 임의 개조 여부를 주기적으로 탐지하고, 탐지된 경우 서비스 이용을 제한하도록 보안 기능이 적용되어야 한다.

- **(앱 무결성 검증)** 앱 코드, 데이터, 리소스 파일 등에 대해 무결성을 검증하여야 하며, 필요시 거래 이체 등 중요시점에서 주기적으로 검증하여야 한다.
- **(악성코드 위협 대응)** 악성코드 감염 여부를 전자금융서비스 앱이 실행되는 동안 중요 시점에 검사 및 대응할 수 있는 기능을 제공하여야 한다.
- **(암호 적용)** 통신구간 중요정보 암호 적용 시, 암호키 관리, 암호 알고리즘, 암호 프로토콜, 사용하는 암호 알고리즘 및 프로토콜의 조합 등의 안전성을 고려하여야 한다.
- **(통신 구간의 암호화)** 통신구간에서 암호화하여 정보가 유출되지 않아야 한다.
- **(중요정보의 암호화)** 개인정보 또는 금융거래정보는 스마트폰 입력단부터 금융회사 전자금융 서버까지 전 통신구간을 암호화하여 전송하여야 한다.
- **(거래전문 무결성 검증)** 거래전문에 대한 해쉬값 검증 등 무결성을 검증하여야 한다.
- **(인증서 유효성 검증)** 금융앱에서 안전한 통신을 위해 SSL(Secure Socket Layer) 등을 이용하는 경우, 서버 인증서의 유효성 검증(서버주소, 유효기간, 발급기관, 소유자 등)을 수행하여야 한다.
- **(암호키 관리)** 암호 키 생성, 설정, 저장, 유효기간, 분배, 복구 및 파기 등의 계획을 수립하고 안전하게 관리하여야 한다.

3. 앱 보안성 확인

스마트폰 전자금융서비스 앱 개발을 완료하면, 금융회사는 최초 기획·설계 시 정의한 요구사항에 대한 보안성을 확인하여야 한다.

- **(보안기능 확인)** 개발이 완료된 앱이 기획 및 설계단계에서 정의한 기능과 요구사항이 충족되었는지 확인하여야 한다.
- **(보안성 확인)** 개발이 완료된 앱은 자체 테스트 절차(정적테스트*, 동적테스트** 등)를 통해 보안성이 확인되어야 하며, 앱과 관련 IT 시스템에 대한 보안성 확인절차가 마련되어야 한다.

* 정적테스트 : 앱을 실행하지 않고 소스코드 등에서 결함을 찾아내는 테스트 방법

** 동적테스트 : 앱을 실행한 상태에서 결함을 찾아내는 테스트 방법

> ☞ 보안성 확인 예시 : 설정파일, 서버주소 등 중요정보 노출 여부 확인, 메모리상에서 암호키 등 중요 데이터 노출 확인

4. 안전한 앱 배포

금융회사는 전자금융서비스 앱의 서명에 이용한 인증서는 안전하게 관리하여야 하며, 이용자에게 제공하는 앱은 공식 배포처를 이용하여 검증된 앱을 배포하여야 한다.

- **(배포 인증서 관리)** “앱” 서명에 이용되는 금융회사의 배포 인증서는 사내의 인증서를 저장하는 서버 또는 전용 단말기 등에서 관리되어야 하며, 노출 또는 유포되지 않도록 하여야 한다.
- **(안전한 앱 배포)** 금융회사는 원칙적으로 공식 배포처*를 이용하여 검증된 금융 앱을 배포하여야 한다.

  * 앱 배포 시 애플 앱 스토어, 구글 플레이 스토어 등 스마트폰의 보안수준을 낮추지 않아도 정상적으로 앱 설치가 가능한 검증된 배포처

  〖 참고 〗 [부록 2] 안전한 스마트폰 전자금융서비스 배포방안

5. 앱 업데이트 관리

안전한 스마트폰 전자금융서비스를 위해, 공식 배포처에 앱 등록 후에도 앱에 대한 기능 및 보안성을 확인하는 등 지속적인 업데이트 관리가 이루어져야 한다.

- **(기능변경 시 검증)** 기능변경 시 앱에 대한 보안성 확인절차(정적·동적 테스트)를 수행하여야 한다.
- **(앱 업데이트 관리)** 스마트폰 전자금융서비스 앱의 중요기능에 대해서는 주기적으로 보완조치를 수행하고, 중요기능이 적용된 앱에 대해서는 스마트폰 이용자로 하여금 업데이트 설치를 유도하여 안전한 서비스를 이용할 수 있도록 해야 한다.

> ☞ 보완 조치 예시 : 루팅·탈옥 탐지, 무결성 검증 등 중요기능에 대해서 주기적으로 보안기능을 강화하여 업데이트 수행

6. 설치·실행환경 관리

이용자가 안전한 환경에서 스마트폰 전자금융서비스 앱을 설치·실행할 수 있도록, 스마트폰 보안설정 변경 금지, 운영체제 임의개조 탐지, 악성코드 검사 등 보안방안을 제공하여 이용자의 스마트폰 환경을 관리하여야 한다.

- **(보안설정 변경 금지)** 앱 설치 시 "알 수 없는 출처(소스) 허용"*등 이용자의 스마트폰 보안수준을 변경하지 않도록 해야 한다.
  * 안드로이드 운영체제를 탑재한 스마트폰의 경우, '알 수 없는 출처(소스) 허용' 시 보안수준이 변경됨
- **(운영체제 임의 개조 탐지 및 이용제한)** 스마트폰 운영체제의 임의 개조 여부를 탐지하고, 탐지된 경우 서비스 이용을 제한하도록 한다.
- **(악성코드 위협 대응)** 악성코드 감염 여부를 앱이 실행되는 동안 중요시점에 검사 및 대응할 수 있는 기능을 제공하여야 한다.
- **(이용자 정보수집 최소화)** 개인정보 등 이용자 정보 수집 시 사전에 동의를 구하고, 최소한의 정보*만을 수집하여야 한다.
  * 금융거래 정보와 같은 금융사고 발생 시 추적성 강화를 위한 정보 등은 필요시 『개인정보보호법』에 따라 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다.

7. 앱 무결성 검증

악의적인 목적으로 위·변조된 스마트폰 전자금융서비스 앱이 실행되는 것을 방지하기 위해서 이용자에게 제공하는 앱의 무결성을 검증하여야 한다.

■ **(앱 무결성 검증)** 앱 코드, 리소스 파일 등에 대해 무결성을 검증* 하여야 하며, 필요시 거래 이체 등 중요시점에서 주기적으로 검증하여야 한다.

* 키교환 및 안전성이 검증된 표준 암호화 알고리즘을 통해 무결성 정보를 생성 및 서버에서 검증할 수 있어야 한다.

[스마트폰 전자금융서비스 안전대책 체크리스트]
- 앱 무결성 검증 포함-

영역	점검항목	세부내용
스마트폰 금융 보안대책	백신프로그램 적용	① 앱 실행 시 백신프로그램 구동 여부 (안드로이드 운영체제를 탑재한 스마트폰의 경우 해당)
		② 백신프로그램 최신버전 업데이트 여부 (안드로이드 운영체제를 탑재한 스마트폰의 경우 해당)
	입력정보 보호 대책 적용 여부	③ 주요정보 입력시 입력정보 보호 대책 적용 여부 (가상 보안키패드 등)
	금융정보 종단간 암호화 적용 여부	④ 스마트폰 앱과 금융회사 전자금융 서버간의 종단간 암호화(End-to-End) 적용 여부
	거래전문 무결성 검증기법 적용	⑤ 거래정보 무결성 정보생성 및 검증 여부
		⑥ 표준 통신규약 적용 여부
앱 위·변조 방지대책	폰 임의개조 탐지 및 차단 적용	⑦ 스마트폰 앱 실행시 폰 임의개조 탐지 및 차단 여부

	앱 무결성 검증기술 적용	⑧ 앱 구동시 설치파일, 바이너리 파일, 리소스 파일 등 중요 파일 무결성 정보생성 및 무결성 검증 여부
		⑨ 암호기술 (적용알고리즘/키공유 방식)의 적정성
	코드(모듈)보호	⑩ 실행 코드 보호 대책 적용 여부 - 코드보호 기술 적용 (난독화, 암호화 등) - 네이티브 라이브러리 구현 - 코드/모듈 업데이트
기타	앱 취약점 점검	⑪ 위·변조 방지모듈에 대한 취약점 점검 여부 (자체 또는 전문기관 위탁)
	위·변조 앱 모니터링	⑫ 위·변조 앱 유통에 대한 대응의 적정성
	앱 위·변조 로그기록	⑬ 앱 위·변조 앱에서 접속 시도시 로그기록 보관 여부
	멀티로그인 (Multi-Login) 차단	⑭ 동시에 2대의 스마트폰(PC와 스마트폰)에서 동일ID로 접속 허용 여부
	스마트폰에 중요정보 저장 금지	⑮ 스마트폰에 중요 금융정보의 저장 여부
	스마트폰 금융거래기록 정보 보관	⑯ 금융사고 발생시 추적성 강화를 위해 스마트폰 금융거래 정보 보관 여부

[참고]

· '스마트폰 금융 안전대책 이행실태 점검 체크리스트', 금융감독원,

· [부록 1] 제2절 스마트폰 전자금융서비스 안전대책 점검방법

8. 이용자 확인 강화

스마트폰 전자금융서비스에서 이용자 본인 여부 확인 및 다중접속에 대한 관리 등 안전한 이용자 확인에 대한 통제방안을 마련하여야 한다.

■ **(이용자 확인)** 스마트폰 전자금융서비스 신규 가입 시에는 이용자 신원확인*을 거쳐야 한다.

* 신규 가입 시 영업점 방문이 필요한 경우에는 계좌개설, 실명확인 등을 거쳐 인터넷뱅킹서비스 가입한 고객으로서 스마트폰에서 '스마트폰 전자금융서비스' 가입절차를 거친 이용자에 한하여 서비스 제공

■ **(서비스 가입절차 강화)** 스마트폰 전자금융서비스 가입 시, 다단계 가입자 확인을 통해 서비스 가입 절차를 강화하여야 한다.

☞ 서비스 가입절차 강화 예시 : 2개 이상 방안을 조합하여 다단계 가입자 확인
- 방안① (지식기반 인증수단) : 사용자가 가진 지식이나 알고 있는 정보를 확인하여 인증하는 방식
  예시) 비밀번호 등
- 방안② (소유기반 인증수단) : 소지한 인증수단인 토큰을 이용하여 인증하는 방식
  예시) 보안카드, OTP 토큰 등
- 방안③ (생체기반 인증수단) : 사용자가 가진 특징을 이용하는 인증방식
  예시) 지문, 홍채 등

■ **(멀티로그인 관리)** 스마트폰을 이용한 다중접속 관리* 등의 기능을 마련하여 이용자 확인 기능을 강화하여야 한다.

☞ 멀티로그인 관리 예시 : 동일 ID로 PC와 스마트폰 또는 동시에 2대 이상의 PC와 스마트폰에서 접속하는 등 멀티로그인을 제어

9. 안전한 통신

스마트폰 전자금융서비스에서 통신구간의 암호화, 중요정보의 암호화 적용, 거래전문의 무결성 검증 등 통신영역에 대한 보호대책을 마련하여야 한다.

■ **(암호 적용)** 통신구간 중요정보 암호 적용 시, 암호키 관리, 암호 알고리즘, 암호 프로토콜, 사용하는 암호 알고리즘 및 프로토콜의 조합 등의 안전성을 고려하여야 한다.

〖 참고 〗 [부록 1] 제3절 전송정보 암호화

□「금융부문 암호기술 관리 가이드」, 금융보안연구원, 2010.1
□「암호 알고리즘 및 키 길이 이용 안내서」, 미래창조과학부, 한국인터넷진흥원, 2013.1
□「Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lenghts」, NIST Special Publication 800-131A, 2011.1
□「Recommendation for key Management Part1:General(Revision3)」, NIST Special Publication 800-57, 2012.7

- **(통신 구간의 암호화)** 통신구간에서 암호화하여 정보유출에 대비하여야 한다.
- **(중요정보의 암호화)** 개인정보 또는 금융거래정보는 스마트폰 입력단부터 금융회사 전자금융 서버까지 전 통신구간에 있어 별도로 암호화하여 전송하여야 한다.

☞ 안전한 암호화 구현 방안 예시 :
· 개인정보 또는 금융거래정보의 암호화에 이용되는 입력단 관련 암호 모듈은 암호화 기능만 제공.
  - [금융앱] 암·복호화 함수제공 예시 : 개인정보 또는 금융거래정보의 암호화 함수 A,
  - [금융회사] 암·복호화 함수제공 예시 : 개인정보 또는 금융거래정보의 복호화 함수 AA

[참고] 『종단간 (End-to-End) 암호화 적용 가이드』,금융보안연구원, 2007.10

- **(거래전문 무결성 검증)** 표준 보안프로토콜(SSL 등), 해쉬 알고리즘(HMAC* 등) 등을 이용하여 거래전문에 대해 무결성을 검증할 수 있어야 한다.

  * HMAC : Keyed-Hashing for Message Authentication Code

- **(서버 인증서 유효성 검증)** 금융 앱에서 안전한 통신을 위해 SSL(Secure Socket Layer) 등의 암호화 통신을 이용하는 경우, 서버 인증서의 유효성 검증(서버주소, 유효기간, 발급기관, 소유자 등)을 수행하여야 한다.

10. 이용자 교육

스마트폰 전자금융서비스 이용 시 이용자의 보안인식 부족 등으로 발생할 수 있는 위협을 사전에 방지하기 위하여, 안전한 스마트폰 전자금융서비스 이용에 대한 유의사항을 홍보하고 지속적인 이용자 교육이 이루어져야 한다.

- **(이용자 교육·홍보)** 이용자의 안전한 스마트폰 전자금융서비스 이용을 위해 교육 및 홍보가 이루어져야 한다.
- **(이용자 유의사항)** '스마트폰 전자금융서비스 이용자 단계별 보안 유의사항'을 참고하여 이용자의 보안 인식을 제고할 수 있다.

[스마트폰 전자금융서비스 이용자 단계별 보안 유의사항]

[설치단계 유의사항]

① 스마트폰 사용 환경을 임의로 변경(루팅, 탈옥 등)하지 않기

② 공식 앱 스토어(애플 앱 스토어, 구글 플레이 스토어, 통신사 스토어 등)를 이용하여 금융 앱을 설치하기

③ SMS, 이메일, 인터넷 등 출처가 확인되지 않은 링크를 클릭하지 않기

④ 스마트폰의 보안설정 중 '알 수 없는 출처(소스)'*를 V체크하지 않기

* 안드로이드 운영체제를 탑재한 스마트폰의 경우 해당

[이용단계 유의사항]

① 보안승급 서비스를 사칭하여 계좌번호, 보안카드번호 등 금융정보를 요구하는 경우 입력하지 않기

② 스마트폰이나 인터넷에 보안카드번호 등 금융정보 저장하지 않기

[관리단계 유의사항]

① 피싱, 파밍, 스미싱 등 피해 발생 시 **경찰청(112), 금융회사 콜센터, 금감원 피싱신고센터(1332)**로 신고하여 즉시 지급정지 요청하기

② 스마트폰 교체·수리 전 중요정보 삭제하기

③ 스마트폰 분실·도난 시 금융서비스 사용중지 신청하기

④ 스마트폰 운영체제 및 금융 앱을 최신버전으로 업데이트 하기

⑤ 스마트폰 악성코드 검사하기

[참고]

· [부록 3] 스마트폰 전자금융서비스 관련 이용자 유의사항

☐ 금감원, 스마트폰 금융거래 10계명
☐ 금감원, 스미싱 피해예방 요령
☐ 경찰청 사이버테러대응센터, 스미싱 피해 예방 7가지 수칙
☐ KISA, 스마트폰 이용자 10대 안전수칙

11. 시스템 보안

스마트폰 전자금융서비스에서 금융정보를 처리하는 경우, 거래정보 및 로그 관리 등 전자금융서비스 관련 시스템에 대한 보안 관리가 이루어져야 한다.

- **(거래정보 관리)** 스마트폰 전자금융서비스에서 금융정보 등 중요정보는 가급적 최소화하여 저장 및 관리* 하여야 한다.
  * 금융정보의 보관 필요시, 암호화 하는 등 안전하게 저장하고, 고유식별정보를 처리하는 경우 『개인정보보호법』에 따라 안전성 확보에 필요한 조치를 하여야 한다.
- **(거래기록 보관)** 스마트폰 전자금융 거래기록정보 보관 시 이용자 ID, 거래일시, 거래내역 등을 전자금융업자 5년, 전자금융보조업자 3년간* 보관하여야 한다.
  * 전자금융거래법 제22조(전자금융거래기록의 생성 및 보존),
    전자금융거래법 시행령 제12조(거래기록의 보존기간 및 방법 등)
- **(로그 관리)** 시스템 로그기록은 1년 이상 보존*하도록 하며, 임의개조 및 위·변조 앱에서 접속 시도 등의 로그기록도 보존하도록 조치한다.
  * 전자금융감독규정 제13조(전산자료 보호대책) 제11호, 제18조(IP주소 관리대책) 제3호
- **(보안성 검증)** 전자금융서비스 개시 또는 앱 변경(개편, 기능추가) 전 취약점 점검 등 자체 보안성 검증 및 보완조치 후 서비스를 실시하여야 한다.
- **(내부 서버 시스템 보안 관리)** 내부 서버 시스템 및 서버 보안 프로그램들의 주기적인 보안패치 및 업데이트를 수행하고 주기적인 모의해킹, 취약점 점검 등을 실시하여야 한다.

12. 보안 관리

안전한 전자금융서비스를 위해, 이용자 접속정보 및 서비스 이용내역 제공, 분실·도난 시 대응절차의 마련, 이상금융거래 탐지 시스템 구축 확대 등 서비스 관리가 이루어져야 한다.

■ **(접속 정보 제공)** 스마트폰을 통한 전자금융서비스 로그인 시, 최종 접속 정보 등 이용자가 접속 정보를 확인할 수 있는 기능을 제공하여야 한다.

■ **(서비스 이용내역 제공)** SMS, 앱 기반 Push 서비스* 등을 이용하여 전자금융서비스 거래 내역 등의 정보를 이용자에게 제공하여야 한다.

☞ 서비스 이용내역 제공 예시 : 현행 SMS문자 이외에 앱 기반의 Push메시지를 제공하는 경우 Push메시지 발송 시 암호화하고 수신한 스마트폰 앱에서 복호화
[참고] · [부록 1] 제4절 Push 서비스 구성 및 보안 고려사항 · '푸시(Push) 서비스 제1부 푸시 서버와 서비스 제공자 구간 바이너리 프로토콜 규격', 한국정보통신기술협회 TTAK.KO-06, ('13.3)

■ **(분실·도난 시 대응절차의 마련)** 단말기 분실·도난 관련 사용자 요청 시, 해당 단말기의 전자금융서비스 관련 차단 요청*에 대한 대응 절차를 수립하여 분실·도난으로 인해 발생할 수 있는 사고를 방지하여야 한다.

* 스마트폰에 발급된 모바일 신용카드 사용 중지 등

■ **(이상금융거래 탐지 시스템 구축)** 스마트폰 전자금융서비스에 대해 부정거래 탐지 및 모니터링을 실시함으로써, 금융사고 발생 시 추적성 강화 및 전자금융부정거래를 적시에 효과적으로 대응할 수 있도록 한다.

[참 고 문 헌]

[1] 금융보안연구원, 금융부문 스마트폰 보안 가이드, 2010.12

[2] 금융감독원, 스마트폰 전자금융서비스 안전대책, 2010.1

[3] 금융감독원, 금융권 스마트워크 정보보호 가이드라인, 2011.6

[4] 미래창조과학부, KISA, 모바일 오피스 정보보호 안내서, 2013.12

[5] 안전행정부, KISA, 모바일 대국민 전자정부서비스 앱 소스코드-검증 신청기관을 위한 가이드라인 v4.0, 2014.2

[6] ITU-T, X.1121, Framework of security technologies for mobile end-to-end data communications, 2004.4

[7] ITU-T, X.1122, Guideline for implementing secure mobile systems based on PKI, 2004.4

[8] ITU-T, X.1123, Differentiated security service for secure mobile end-to-end data communication, 2007.11

[9] ITU-T, X.1124. Authentication architecture for mobile end-to-end data communication, 2007.11

[10] ITU-T, X.1125, Correlative Reacting System in mobile data communication, 2008.1

[11] ITU-T X.Sup19, ITU-T X.1120 series, Supplement on security aspects of smartphones, 2013.4

[12] ITU-T, Draft Recommendation X.msec-7, Guidelines on the management of infected terminals in mobile networks, 2013.4

[13] ITU-T, Draft Recommendation X.msec-8, Secure application distribution framework for communication devices, 2013.4

[14] NIST, SP 800-124 Rev.1, Guidelines for Managing the Security of Mobile Devices in the Enterprise, 2013

[15] NIST, SP 800-101 Rev.1, Guidelines on Mobile Device Forensics, 2014

[16] OWASP, Application Security Guide For CISOs, 2013.5
[17] OWASP, Mobile Security Project,
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
[18] ENISA, Smartphones: Information security risks, opportunities and recommendations for users, 2010.12
[19] ENISA, Smartphone Secure Development Guidelines for App Developers, 2011.11

[부 록]

[부록 1] 스마트폰 전자금융서비스 보안 고려사항

[부록 1] 스마트폰 전자금융서비스 보안 고려사항

제1절 프로그램 개발 시 고려사항

1. 프로그램 개발 시 고려사항(플랫폼 공통)

■ **(입력 값 유효성 검증)** 이용자 프로그램에서 입력·전송되는 데이터는 유효성이 검증되어야 한다.

- 텍스트 데이터의 입력·URL을 통해 전달되어지는 데이터·이용자가 제출한 HTML과 같이 신뢰할 수 없는 데이터의 열람 등 비정상적인 입력 값을 통해 예기치 않은 다양한 정보를 취득할 수 있다.

■ **(시간 및 상태 - Race Condition)** 프로세스 간 동시 또는 거의 동시수행을 지원하는 병렬시스템에서 프로세스의 비정상적인 행동을 유도하여 이용자에게 사전에 주어진 권한 이상을 수행하는 취약점에 대한 고려가 필요하다.

■ **(접근통제의 검증)** 프로그램이 이용하는 각종 기능은 적절한 접근 통제 정책을 갖고 있으며 해당 통제가 우회되었을 경우에 대한 대비책이 함께 고려되어야 한다.

- 다른 프로세스 또는 이용자가 쓰기 가능한 위치에 파일이 위치한 경우, 파일 생성 전 파일의 형식·ID·링크 등의 검사가 실패하는 경우, 파일 생성 후 결과 코드가 실패하는 경우 예기치 않은 보안 문제가 발생할 수 있다.

■ **(관리자 상승 권한 기능의 제한)** 관리자권한으로 동작하는 기능을 최소화 하여야 하며 이용자 중요정보(사진·전화번호·SMS메시지·프로그램설정 등)의 수집 또는 수정되는 기능이 포함되어서는 안된다.

■ **(데이터 보호)** 프로그램에서 이용되는 데이터가 각종 비밀정보를 처리하는 경우 운영체제에서 지원하는 암호화 기술을 이용할 수 있도록 해야 한다.

■ **(예외처리에서 중요정보 노출의 제한)** 비정상 데이터(각종 예외처리)를 처리하는 부분에서 이용자의 중요정보 또는 시스템 정보가 노출되지 않도록 해야 한다.

■ **(비인가 API 사용의 제한)** 단말기에 탑재된 운영체제에서 공식으로 지원하는 API만을 이용하여 기능이 동작될 수 있도록 해야 한다.

■ **(상용 API 이용의 검증)** 상용 또는 공개된 API를 이용하여 기능을 구현할 경우 이에 대한 안전성 검증 절차가 마련되어야 한다.

- 상용 API의 경우 해당 회사에 판매하는 보안성이 검증된 최신 버전을 이용하여야 한다.

■ **(임의 파일 업로드의 방지)** 스마트폰을 통한 외부 파일 업로드 기능을 제공하지 않아야 하며, 필요에 의해 제공할 경우 정해진 파일 형태 이외의 파일은 업로드 되지 않도록 해야 한다.

- 외부 파일 업로드 기능이 필요할 경우 전용 디렉토리를 별도로 생성하고 해당 디렉토리의 실행권한을 제거해야 해야 하며, 업로드 가능한 파일의 확장명을 정의하고 해당 파일만이 업로드 되도록 설계 및 구현하여야 한다.

2. Java 계열 프로그램 개발 시 고려사항

■ **(데이터 은닉)** 소프트웨어의 기능 중 중요 데이터를 처리하는 기능에서는 캡슐화(Encapsulation)[1] 기법을 이용하여 의도하지 않는 중요 데이터의 노출을 예방하도록 해야 한다.

■ **(Null 매개변수의 검사)** 일부특정 함수로 기능 구현 시 매개변수 검사를 하지 않는 습관에 의해 예기치 못한 동작이 발생할 수 있으므로 이에 대한 검사를 실시하여야 한다.

- Object.equals(), Comparable.compareTo(), Comparator.compare() 로 구현 시 매개변수를 Null과 비교하여야 한다.

■ **(소프트웨어 구동 정보의 보호)** 안드로이드 계열에서 소프트웨어 구동에 필요한 다양한 정보가 포함된 파일에 대한 보호가 필요하다.

- Manifest.xml에서 “공유아이디 설정의 삭제”·“외부접근 금지 설정” 등을 통해 비정상적인 접근 행위를 방지하여야 한다.

1) 객체의 자료와 행위를 하나로 묶고, 실제 내용을 외부에 감추는 형태의 정보은닉의 개념

3. C/C++, Object-C, C# 계열 프로그램 개발 시 고려사항

■ **(버퍼오버플로우 검증)** 입력 값에 대한 길이 검증을 실시하여 버퍼오버플로우(Buffer Overflow)[2] 등과 같은 해킹 기법이 방어 될 수 있도록 하여야 한다.

- Stack Overflow · Heap Overflow · String Handling · Calculating Buffer Sizes · Avoiding Interger · Format String 등과 같은 다양한 Buffer Overflow 해킹 기법이 존재하고 있다.

■ **(프로세스 간 통신에 대한 검증)** 프로세스와 프로세스 간 데이터를 공유하는 기능을 구현할 경우 데이터 공유 과정(파일, 데이터베이스, 네트워크 연결 등)에서 예기치 않은 공격에 취약할 수 있으므로 이에 대한 고려가 필요하다.

- 다른 프로세스 간 데이터를 전송할 경우 입출력에 유효성을 검사하지 않는 경우가 있어 이에 대한 잠재적 위협에 노출 될 수 있다.

■ **(올바른 포인터의 이용)** 잘못된 포인터[3] 사용으로 인해 소프트웨어 메모리 누수 및 각종 보안 결함이 발생할 수 있으므로 올바르고 적절하게 포인터를 사용하여야 한다.

■ **(검증된 API의 이용)** 문자(열)을 처리를 위해 사용되는 고전 함수(API)에 내제되어 있는 고유취약점이 있으므로, 안전성이 검증된 함수가 이용되도록 해야 한다.

2) 메모리를 처리함에 있어 오류가 발생하여 잘못된 동작을 유도하는 보안 취약점
3) 프로그래밍 언어에서 다른 변수, 혹은 그 변수의 메모리 공간주소를 가리키는 변수를 의미함

제2절 스마트폰 전자금융서비스 안전대책 점검방법

스마트폰 앱 무결성 검증 등의 항목을 포함하여 스마트폰 전자금융서비스 안전대책의 이행은 아래의 점검방법[4]을 참조하시기 바랍니다.

영역	점검방법
스마트폰 금융 보안대책	1. 백신프로그램 적용 o 앱 실행 시 백신프로그램 구동 ※ 안드로이드 운영체제를 탑재한 스마트폰의 경우 해당 o 백신프로그램 업데이트 ※ 안드로이드 운영체제를 탑재한 스마트폰의 경우 해당 - 해당 금융회사에서 제공하는 공개된 최신버전(설치 후 버전 확인)
	2. 입력정보 보호대책 적용 여부 o 주요 금융정보 대상 (기밀성 대상) : 계좌비밀번호, 공인인증서 비밀번호 등 o 해당 필드 클릭 시 가상키패드 등 활성화 및 키패드 위치 변화 여부
	3. 주요 금융정보 종단간 암호화 적용 여부 o 주요 금융정보 대상 (기밀성 대상) : 계좌번호, 계좌 비밀번호, 금액 등 o 종단간 암호화 : 앱(또는 가상키패드)으로부터 서버 간 암호화 유지 여부 예) 앱에서 암호화하고 서버에서 복호화(통신사 등에서 복호화 금지)
	4. 거래전문 무결성 검증 기법 o 표준 보안프로토콜(SSL, HMAC* 등) * HMAC : Keyed-Hashing for Message Authentication Code
앱 위·변조 방지대책	5. 폰 임의개조 탐지 및 차단 o 임의 개조폰에서 앱 실행 시 종료여부
	6. 중요 파일 무결성 검증기술 적용 o 주요 검증대상 파일을 변조 후, 앱을 실행하여 정상적으로 서비스 이용 가능 혹은 제한여부 확인

4) 금융감독원, “스마트폰 금융 안전대책 이행실태 점검 체크리스트”의 체크리스트와 점검방법을 참조하였음

	- 적용된 앱 무결성 검증기술의 특성에 따라 변조대상을 선별하여 점검 진행 o 주요파일 무결성 검증 대상 - 안드로이드 : 설치파일, 실행파일, 리소스파일(xml, 이미지 등) 등 - iOS : 실행파일, 리소스 파일(xml, 이미지 등) 등 o 주요파일 무결성 검증 방법 - 안드로이드 : 설치파일 다운로드 →파일 변조→스마트폰에 주입 및 설치→앱 실행 후 정상적으로 서비스 이용/제한 여부 확인 - iOS : 스마트폰으로부터 변조대상 추출→파일 변조→스마트폰에 주입 →앱 실행 후 정상적으로 서비스 이용/제한여부 확인 ※ iOS 실행파일 변조는 임의개조 폰에서만 가능하며, 순정iOS 최신 버전에서 파일 추출/주입 도구가 정상적으로 동작하지 않을 경우 점검 불가
	7. 코드(모듈) 보호 o 코드보호 기술 적용 - 난독화, 암호화 등 코드보호 기술 적용 여부 o 네이티브 라이브러리 구현 - JAVA가 아닌 해독이 어려운 네이티브 라이브러리로 앱 구현 여부 o 코드/모듈 업데이트 - 앱 코드(모듈)에 자동업데이트 기능이 내장되어 위·변조 앱에서 접속시 자동 업데이트 적용 여부 o 기타
기타	8. 앱 취약점 점검 o 앱에 보안기능 및 위·변조 방지모듈에 취약점 점검을 자체 또는 전문기관 위탁 실시 여부
	9. 위·변조 앱 모니터링 o 블랙마켓 등에서 유통되는 위·변조 앱에 대한 자체 또는 위탁 모니터링 및 발견시 대응 여부
	10. 앱 위·변조 로그 기록 o 임의 개조된 폰에서 접속 시도시 로그기록 보관 여부 o 위·변조 앱에서 접속 시도시 로그기록 보관 여부 ※ 보관 항목 : 이용자ID, 접속일시, HMAC코드, 전화번호, 휴대폰정보 등

	11. 멀티로그인(Multi-Login) 금지 o 스마트폰에서 앱을 실행하여 로그인(ID/PW)상태를 유지하고 다른 스마트폰(또는 PC인터넷뱅킹)에서 동일 ID로 접속 가능 여부
	12. 스마트폰에 주요 금융정보 저장 금지 o 앱 디렉토리에 주요 금융정보 저장 여부
	13. 금융거래기록 정보 보관 o 금융사고 발생시 추적성 강화를 위해 스마트폰 금융거래 정보 보관 여부 * 보관항목 : 이용자ID, 거래일시, 출금계좌, 입금계좌, 전화번호, 휴대폰정보 등

제3절 전송정보 암호화

네트워크를 통해 전송되는 모든 개인정보 또는 금융거래정보는 암호화하여 전송하고 전송구간에서 평문으로 노출되지 않도록 처리한다. 안전한 암호기술 적용을 위해 금융권에서 현재 사용 중인 암호알고리즘을 기반으로 권장되는 암호알고리즘의 종류 및 최소 키 길이를 기술하였다.[5] 아래 기술된 내용 이외에 국내외 주요기관에서 안전성이 검증된 암호알고리즘의 적용도 가능하다[6].

■ 권고하는 국내외 암·복호화용 대칭키 암호 알고리즘은 AES, SEED, ARIA 등이 있으며, 보안 강도별 대칭키 암호 알고리즘은 아래와 같다.

용도	암호알고리즘	키 길이
암·복호화용	3TDEA[7]	168 bit 이상
	AES*	128 bit 이상
	SEED**	128 bit 이상
	ARIA	128 bit 이상

[표 4] 권고 대칭키 암호알고리즘 및 키 길이

* AES-192/256 경우 이론적으로 가능한 공격이 발표되어 추후 안전성에 대한 변화가 예상됨
** SEED-192/256이 발표된 상태이므로 안전성이 검증된 후 키 길이 변화가 예상됨

■ 전자서명, 키 공유, 메시지 암·복호화 등을 위해 사용되는 권고하는 공개키 암호 알고리즘 및 최소 키 길이는 아래와 같다.

용도	암호알고리즘	키 길이
전자서명	RSASSA-PSS	2048 bit 이상

5) 금융보안연구원, 2010.1, “금융부문 암호기술 관리 가이드”와 2010.12, “금융부문 스마트폰 보안 가이드”를 기본으로 하여, NIST, KISA 등 관련 기관에서 권장하는 암호 알고리즘 및 키 길이를 참조하였음
6) 국내 암호알고리즘은 ‘검증대상보호함수(IT보안인증사무국)’와 국내 표준들을 기반으로 구성하며, 그 외의 암호 알고리즘을 사용할 경우, 국외 권고(안)을 참고하기를 권장함
7) 세 개의 키가 다른 TDEA(Triple Data Encryption Algorithm)
8) PKCS#1 v2.0(RSA Cryptography Standard)버전 이상에 포함된 알고리즘을 의미함

	RSASSA-PKCS#1(v1.5)[8]	2048 bit 이상
	ECDSA	224 bit 이상
	EC-KCDSA	224 bit 이상
키 공유 및 메시지 암·복호화용	RSAES-OAEP	2048 bit 이상
	ECDH	224 bit 이상

[표 5] 권고 공개키 암호 알고리즘 및 키 길이

■ 권고하는 해쉬함수는 SHA-2 이상(SHA-224/256, SHA-384/512 등)을 사용하되, HAS-160[9]은 2010년도부터 단순해쉬·전자서명용으로 사용하는 것을 권장하지 않으며, SHA-1[10]은 새로운 어플리케이션에 적용하는 것을 권장하지 않는다.

■ 암호 알고리즘 및 키 길이 선택 시, 암호 알고리즘의 안전성 유지기간과 보안강도 별 암호 암고리즘 키 길이 등을 기반으로 목적에 맞게 암호 알고리즘 및 키 길이를 선택하도록 권장한다.

암호알고리즘 / 보안강도			112 비트	128 비트	192 비트	256 비트
대칭키 암호 알고리즘(키길이)			112	128	192	256
해쉬함수(보안강도)			112	128	192	256
공개키 암호 알고리즘	인수분해(비트)		2048	3072	7680	15360
	이산대수	공개키(비트)	2048	3072	7680	15360
		개인키(비트)	224	256	384	512
	타원곡선암호(비트)		224	256	384	512
암호알고리즘 안전성 유지기간(년도)			2011년에서 2030년까지 (최대20년)	2030년 이후 (최대30년)		

[표 6] 보안 강도별 암호 알고리즘

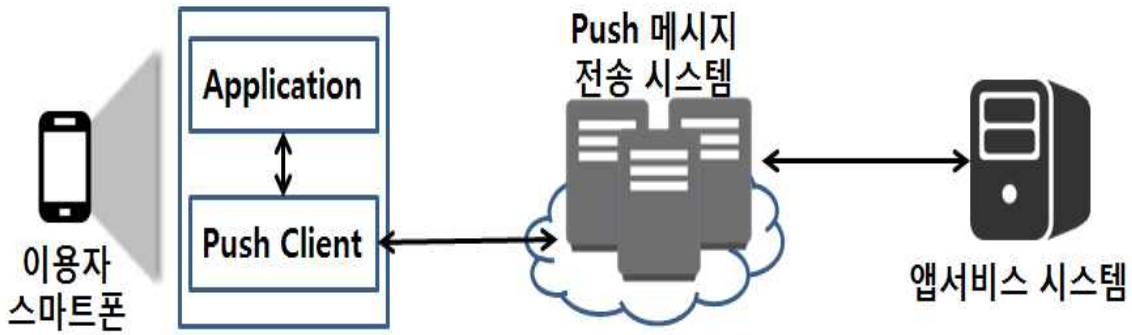
9) HAS-160은 충돌저항성(안전성)이 112bit 보안강도를 제공하지 못하므로, 2010년도부터 단순해쉬·전자서명용으로 사용하는 것을 권장하지 않음(출처 : KISA, 2013.01 제·개정, “암호 알고리즘 및 키 길이 이용 안내서”)

10) SHA-1은 충돌저항성(안전성)이 80bit 보안강도 이하를 제공하여, 새로운 어플리케이션에 적용하는 것을 권장하지 않음(출처 : KISA, 2013.01 제·개정, “암호 알고리즘 및 키 길이 이용 안내서”)

제4절 앱 기반 Push 서비스 구성 및 보안 고려사항

1. 앱 기반 Push 서비스 구성

금융회사는 SMS외에도 Push 서비스를 이용하여 전자금융서비스 거래 내역 등의 정보를 이용자에게 제공할 수 있다. 이러한 Push 서비스는 일반적으로 앱 서비스(예 : 전자금융서비스 앱) 시스템에서 Push 메시지 전송 시스템을 통해 이용자에게 제공된다.



<그림 4> 앱 기반 Push 서비스의 일반적 구조

Push 서비스는 Push 메시지 전송시스템의 구축 방식에 따라, Public Push 서비스와 Private Push 서비스로 구분할 수 있다.

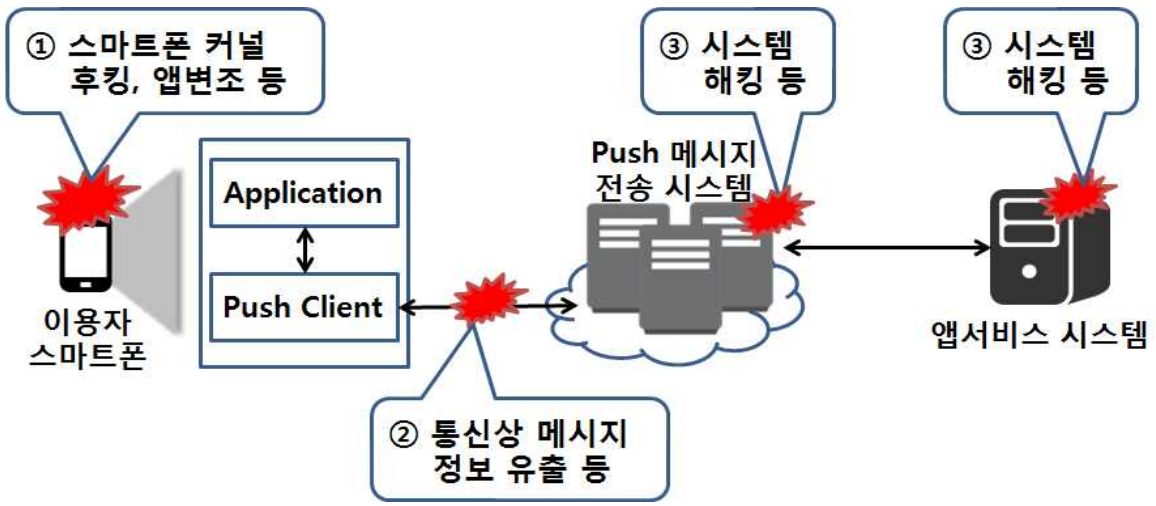
구분	내용
Public Push	외부에 구축되어 있는 Push 메시지 전송 시스템 및 서비스 활용 ※Google사(GCM, Google Cloud Messaging service), Apple사(APNS, Apple Push Notification service), 국내 통신사 등
Private Push	금융회사 내부에 Push 메시지 전송시스템을 구축

[표 7] 앱 기반 Push 서비스 구분

2. 앱 기반 Push 서비스 구축 시 보안 고려사항

기존 SMS서비스에 비해 Push 서비스는 앱 간(타 앱과 전자금융서비스 앱 등) 내부 데이터 접근이 불가능하여 메시지 탈취, 삭제 등이 어려운 장점이 있으나, Push 서비스 시스템 해킹, 통신 시 메시지 정보 유출 등 다양한 보안적 측면을 고려하여 서비스를 제공하여야 한다.

※ SMS 서비스의 경우, 공격자가 이용자 스마트폰의 SMS 관련 권한을 탈취하면 SMS 메시지 탈취, 삭제 등이 가능함



<그림 5> 앱 기반 Push 서비스의 보안 위협

① 사용자별 Push ID 저장 등 Push 메시지 전송 및 앱서비스 시스템에 대한 보안 강화 적용 필요

※ ASP(Application Service Provider) 서비스 이용 시 시스템 보안 수준 검토 필요

② 통신 시 Push 메시지 유출 등을 방지하기 위한 메시지 및 통신구간 암호화 등 보안 방안 적용 필요

③ 안전한 중요 정보(Push ID 등) 저장, 신뢰된 이용자 단말기 인증 등을 위한 보안 방안(중요 정보 추출 및 활용 방지 방안, 위·변조 방지 방안 등) 적용 필요

[부록 2] 안전한 스마트폰 전자금융서비스 배포 방안

[부록 2] 안전한 스마트폰 전자금융서비스 배포 방안

1. 공식 앱 배포처가 아닌 경우의 위협

○ 공식 앱 배포처*가 아닌 금융회사 서버, 홈페이지 등을 통해 앱을 배포할 경우, 이용자는 앱 설치 시 '알 수 없는 출처' **설정을 체크해야 함

- '알 수 없는 출처' 기능을 허용할 경우, 이용자 스마트폰의 보안 위협이 높아질 가능성이 존재함

* 앱 배포 시 애플 앱 스토어, 구글 플레이 스토어 등 스마트폰의 보안수준을 낮추지 않아도 정상적으로 앱 설치가 가능한 검증된 배포처

** 안드로이드 운영체제를 탑재한 스마트폰의 경우 해당

<그림 6> '알 수 없는 출처' 기능 예

2. 공식 앱 배포처를 이용한 배포 및 업데이트 방안

○ **(배포 방안)** 공식 앱 배포처를 통해 배포하도록 하며, 금융사 홈페이지 등에서도 안내 등을 통해 공식 앱 배포처를 통해 앱을 설치할 수 있도록 서비스를 제공하여야 함

- 공식 앱 배포처를 통한 배포

<구글 플레이스토어를 통한 설치>

<앱 스토어를 통한 설치>

<통신사 스토어를 통한 설치>

- 스마트폰에서 금융사 홈페이지에서 다운로드 웹 페이지 안내 시

① 다운로드 웹페이지 안내

② 검증된 배포처로 연동

- QR코드 서비스 제공 시

① 금융회사 홈페이지의 QR코드

② QR코드 스캔 후 검증된 배포처로 연동

○ **(업데이트 방안)** 스마트폰 전자금융서비스 앱 프로그램 업데이트 시에도 공식 앱 배포처를 통해 수행할 수 있도록 배포 방안과 동일하게 업데이트 안내 페이지에 앱 스토어 연동

[부록 3] 스마트폰 전자금융서비스 이용자 유의사항

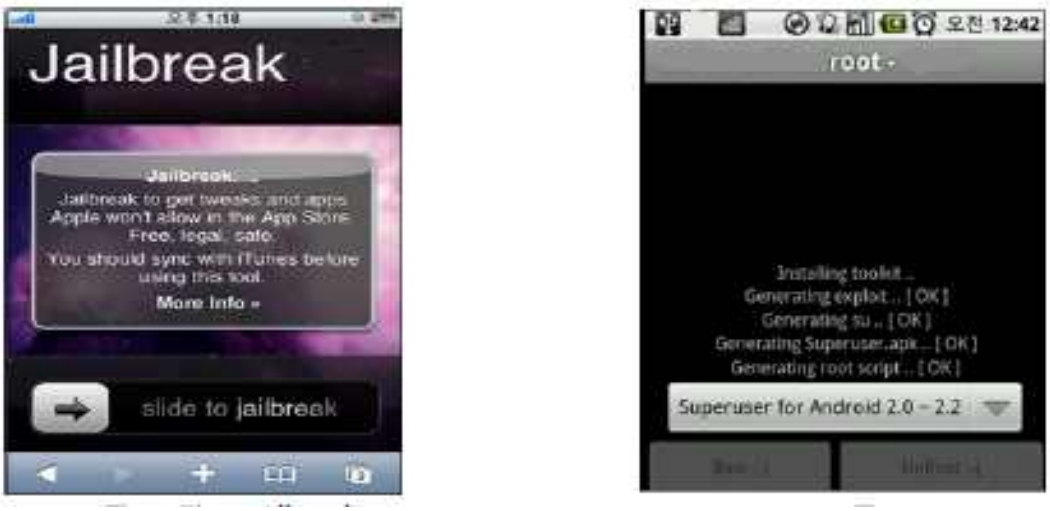
[부록 3] 스마트폰 전자금융서비스 이용자 유의사항

제1절 설치단계 유의사항

1 스마트폰 사용 환경을 임의로 변경(루팅, 탈옥)하지 않기

o 스마트폰 보안에 영향을 주는 구조변경(‘루팅’ , ‘탈옥’ 등)을 하지 마세요.

- 스마트폰의 사용자화면 변경, 성능향상, 비공식 운영체제 설치 등을 위해 아이폰의 탈옥(Jailbreak), 안드로이드의 루팅(Rooting) 등과 같이 제조사에서 제공하는 순정상태의 사용환경을 인위적으로 변경할 수 있는 방법들이 배포되고 있습니다.
- 그러나, 스마트폰의 사용환경을 인위적으로 변경할 경우 보안수준이 낮아지게 되어 문제가 발생할 수 있으므로 순정상태로 사용해야 합니다.



<그림 7> 루팅, 탈옥 예

2 공식 앱 스토어(애플 앱스토어, 구글 플레이스토어, 통신사 스토어 등)를 이용하여 금융 앱 설치하기

○ 안전한 앱 스토어(애플 앱스토어, 구글 플레이스토어, 통신사 스토어 등)를 통해 스마트폰 뱅킹 앱 프로그램을 설치하세요.

- 스마트폰 뱅킹 앱 프로그램을 가장한 악성 프로그램이 설치될 경우, 개인정보가 유출될 수 있습니다.
- 금융회사 홈페이지, 콜센터에서 안내하는 공식 배포처*를 확인하여 해당 금융회사의 스마트폰 뱅킹 앱 프로그램을 다운받아 설치해야 합니다.

* 공인된 앱 스토어(구글Play, 앱스토어, 통신사 스토어 등) 등

<그림 8> 금융 앱 설치 안내 화면 예

3 SMS, 이메일, 인터넷 등 출처가 확인되지 않은 링크를 클릭하지 않기

o SMS, 이메일, 인터넷, 블로그, 게시판 등 출처가 확인되지 않은 링크를 클릭하지 않도록 하고, 인터넷 상에서 apk파일을 다운받아 스마트폰에 저장하지 마세요.

- 스마트폰 전자금융서비스 앱을 가장한 악의적인 프로그램으로 인한 피해를 방지하기 위해 다음과 같은 경로로 전달받은 프로그램은 설치 및 저장하지 말아야 합니다.
  - 메신저, 웹하드, 인터넷카페, 블로그, 게시판 등을 통해 배포되거나, 확인되지 않은 경로로 전달받은 프로그램
  - 사용 환경이 변경된(탈옥, 루팅) 스마트폰에서 실행 가능하도록 변조된 프로그램
  - 확인되지 않은 발송자에게 전달받은 문자메시지에 포함된 설치경로(URL)로 링크된 프로그램 등

<그림 9> SMS 링크(URL) 예

4 스마트폰의 보안설정 중 '알 수 없는 출처'를 V체크 하지 않기

o 확인되지 않은 앱 프로그램이 함부로 설치되지 않도록 '알 수 없는 출처'* 설정을 해제하세요.

* 안드로이드 운영체제를 탑재한 스마트폰의 경우 해당

- '알 수 없는 출처' 설정을 체크할 경우, 사용자의 의식 없이 확인되지 않는 경로로 전달받은 프로그램이나 확인되지 않은 발송자에게 전달받은 문자메시지에 포함된 설치경로(URL)로 링크된 프로그램 등 악의적인 프로그램이 설치될 수 있어 이러한 프로그램의 설치를 원천적으로 차단하여야 합니다.
- 보안 설정 방법(안드로이드의 경우)
  - 환경설정>보안>디바이스 관리> '알 수 없는 출처'에 V체크가 되어 있다면 해제 및 "앱 설치 전 확인"을 체크

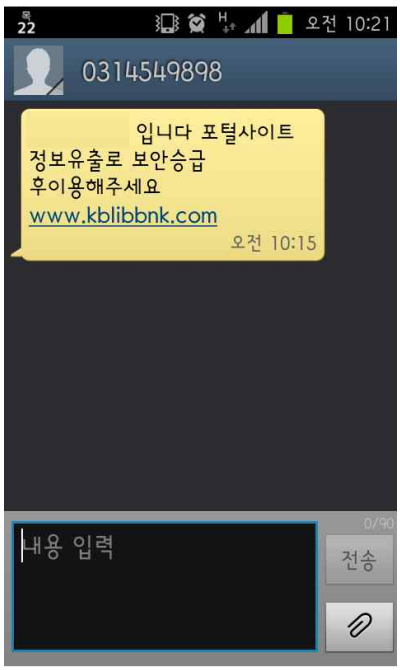
<그림 10> 안드로이드 운영체제 보안설정 예

제2절 이용단계 유의사항

1 보안승급 서비스를 사칭하여 계좌번호, 보안카드번호 등 금융정보를 요구하는 경우 입력하지 않기

o 보안승급 및 업데이트를 명목으로 요구하는 보안카드번호 등 금융정보는 입력하지 마세요.

- 금융회사는 거래인증 목적 이외에 보안승급 및 업데이트 명목으로 이용자의 보안카드번호 등 금융정보를 요구하지 않습니다.
- 문자메세지를 통해 금융회사를 사칭하여 확인되지 않은 경로로 접속을 유도하거나 스마트폰 뱅킹 앱 프로그램 이용 시 금융정보를 요구하면 금융사기를 의심하고 즉시 금융회사 콜센터에 문의하시기 바랍니다.



<그림 11> 보안승급 등 금융회사 사칭 예

2 스마트폰이나 인터넷에 보안카드번호 등 금융정보 저장하지 않기

o 계좌번호, 계좌 비밀번호, 보안카드번호 등 금융정보는 스마트폰이나 인터넷(E-Mail함, 웹하드 등)에 저장하지 마세요.

- 전자금융거래의 이용편의를 위해 스마트폰이나 인터넷(E-Mail함, 웹하드, 트위터 등)에 로그인 아이디·비밀번호, 계좌번호·비밀번호, 보안카드번호, 신용카드번호 등의 금융 정보를 텍스트 또는 이미지 파일형태로 보관하는 경우가 있습니다.
- 그러나 이러한 금융정보는 스마트폰의 분실, 바이러스 감염 등을 통해 저장된 정보가 유출될 수 있으므로, 스마트폰이나 인터넷에 어떠한 형태로도 금융정보를 저장하지 않아야 합니다.

<그림 12> 금융정보 저장 예

제3절 관리단계 유의사항

1 피싱, 파밍, 스미싱 등 피해 발생 시 경찰청(112), 금융회사 콜센터, 금감원 피싱신고센터(1332)로 신고하여 즉시 지급정지 요청하기

o 금융회사를 사칭하거나 피싱 사이트로 연결되는 악성 앱 등에 금융정보를 입력했거나 피해가 발생한 경우, 즉시 관련 기관에 신고하여 사기계좌의 지급정지를 요청하세요.

- 경찰청(112)
- 금감원 피싱 신고센터(1332)
- 금융회사(콜센터) : 금융회사 콜센터는 각 금융사 홈페이지의 사고신고 안내 부분을 참조하세요.

2 스마트폰 교체·수리 전 중요정보 삭제하기

o 스마트폰을 교체하거나 수리하기 전에 공인인증서와 전자금융서비스 앱을 삭제하세요.

- 스마트폰에 설치된 공인인증서와 스마트폰 전자금융서비스 앱은 암호화 등에 의해 보호되고 있습니다.

- 그러나 잠재적인 보안사고를 예방하기 위해서는 스마트폰을 교체하여 타인에게 양도하거나 수리를 맡기기 전에 공인인증서와 스마트폰 전자금융서비스 앱을 삭제해야 합니다.

※ 스마트폰에 저장된 공인인증서를 삭제하더라도 금융회사에서 PC를 통해 발급받았던 공인인증서는 폐지되지 않기 때문에 다시 스마트폰 금융거래를 이용할 경우 PC나 USB에 저장된 공인인증서를 스마트폰으로 재전송하여 사용가능합니다.

o 스마트폰에 모바일 신용카드가 발급되어 있는 경우 카드사에 연락하여 사용중지를 요청하세요.

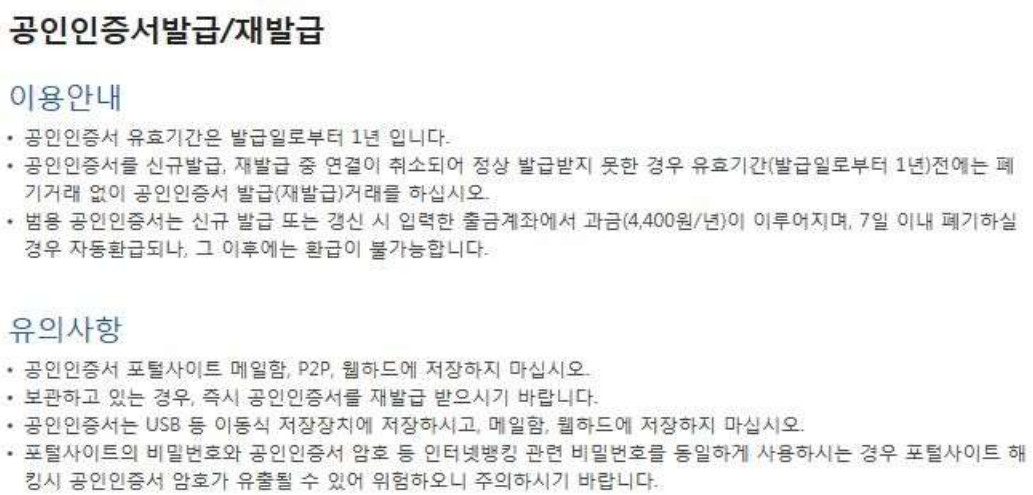
- 스마트폰에 모바일 신용카드가 발급되어 있을 경우에는 발급한 카드사에 연락하여 모바일 신용카드의 사용중지(또는 사용해지)를 요청해야 합니다.

3 스마트폰 분실·도난 시 스마트폰 금융서비스 사용중지 신청하기

o 스마트폰을 분실하거나 도난을 당한 경우 새로운 공인인증서로 재발급 받으세요.

- 스마트폰을 분실하거나 도난을 당한 경우에는 스마트폰에 저장된 공인인증서 및 모바일카드가 악용될 수 있습니다.
- 따라서 스마트폰 전자금융서비스 앱이 설치된 스마트폰을 분실하거나 도난당한 경우에는 공인인증서를 발급받은 금융회사 홈페이지(인증센터)를 통해 새로운 공인인증서를 재발급*해야 합니다.

* 공인인증서를 재발급할 경우, 신규 공인인증서의 비밀번호는 이전에 사용했던 공인인증서 비밀번호 및 계좌 비밀번호와는 다르게 설정해야 하며, 생일, 전화번호, 동일숫자('0000'), 연속숫자('1234') 등과 같이 타인이 알기 쉬운 번호로 사용해서는 안 됩니다.



공인인증서발급/재발급

이용안내

- 공인인증서 유효기간은 발급일로부터 1년 입니다.
- 공인인증서를 신규발급, 재발급 중 연결이 취소되어 정상 발급받지 못한 경우 유효기간(발급일로부터 1년)전에는 폐기거래 없이 공인인증서 발급(재발급)거래를 하십시오.
- 범용 공인인증서는 신규 발급 또는 갱신 시 입력한 출금계좌에서 과금(4,400원/년)이 이루어지며, 7일 이내 폐기하실 경우 자동환급되나, 그 이후에는 환급이 불가능합니다.

유의사항

- 공인인증서 포털사이트 메일함, P2P, 웹하드에 저장하지 마십시오.
- 보관하고 있는 경우, 즉시 공인인증서를 재발급 받으시기 바랍니다.
- 공인인증서는 USB 등 이동식 저장장치에 저장하시고, 메일함, 웹하드에 저장하지 마십시오.
- 포털사이트의 비밀번호와 공인인증서 암호 등 인터넷뱅킹 관련 비밀번호를 동일하게 사용하시는 경우 포털사이트 해킹시 공인인증서 암호가 유출될 수 있어 위험하오니 주의하시기 바랍니다.

<그림 13> 공인인증서 재발급 안내 예

o 스마트폰에 모바일 신용카드가 발급되어 있는 경우 카드사에 연락하여 사용중지를 요청하세요.

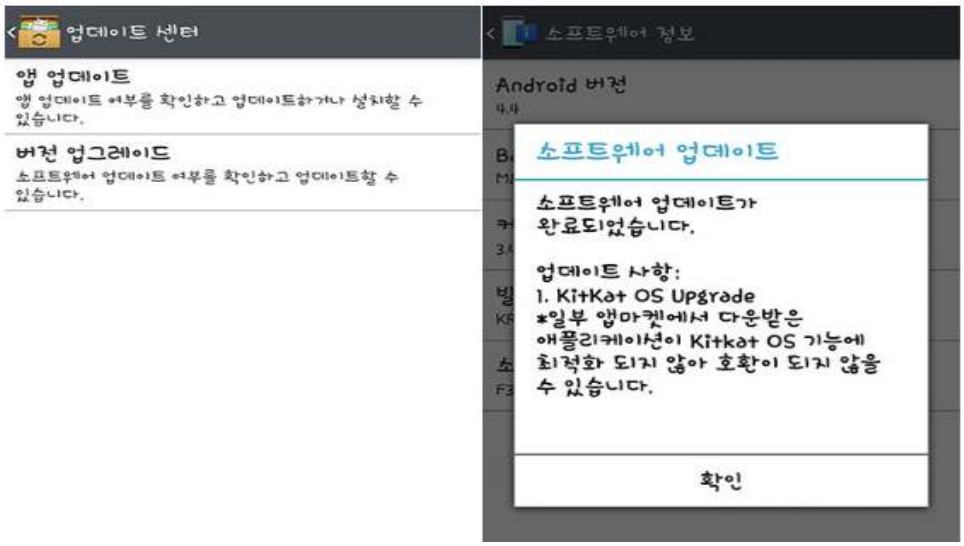
- 분실하거나 도난을 당한 스마트폰에 모바일 신용카드가 발급되어 있을 경우, 즉시 발급한 카드사에 전화(또는 서면)로 신고하여 모바일 신용카드의 사용중지(또는 사용해지)를 요청해야 합니다.
- 모바일 신용카드 이용고객이 사고 신고를 한 경우 신고 접수일로부터 60일전 이후에 발생한 제3자의 부정사용 금액에 대해서는 이용고객에게 과실이 있는 경우를 제외하고 카드사로부터 보상을 받을 수 있습니다.

4 스마트폰 운영체제 및 금융 앱을 최신버전으로 업데이트 하기

o ‘스마트폰 운영체제’, ‘스마트폰 전자금융서비스 앱’을 최신버전으로 업데이트 하세요.

- 스마트폰 제조사에서 제공하는 운영체제의 최신버전을 통해 기존에 확인된 보안취약점에 대한 조치가 가능하므로 최신버전 제공여부를 확인하여 업데이트해야 합니다.

<그림 14> 스마트폰 운영체제 업데이트 안내 예(iTunes 사용)



<그림 15> 스마트폰 운영체제 업데이트 안내 예(스마트폰에서 실행)

o 금융회사에서 제공하는 스마트폰 전자금융서비스 앱도 최신버전으로 업데이트 하세요.

5 스마트폰 악성코드 검사하기

o 수시로 악성코드를 검사하세요.

- 바이러스 등 악성프로그램으로 인한 피해를 줄이기 위해 다음과 같은 경우 악성코드 검사를 위한 전용프로그램을 이용하여야 합니다.
  - 스마트폰을 이용하여 웹하드 또는 홈페이지 등에 접속한 경우
  - 인터넷이나 PC로부터 프로그램 및 파일을 다운로드한 경우
  - 스마트폰이 오작동하거나 저장정보가 삭제된 경우 등

<그림 16> 악성코드 검사 예

- 악성코드 검사 전용 프로그램은 최신버전으로 업데이트해야 새로운 악성코드를 검사할 수 있습니다.

<그림 17> 악성코드 검사 전용 프로그램 업데이트 예

이 “스마트폰 전자금융서비스 보안 가이드” 작성을 위해
다음 분들께서 수고하셨습니다.

2014년 7월

총괄 책임자	금융보안연구원		
	정보보안본부	본 부 장	성 재 모
참여연구원	보안기술연구팀	팀 장	임 형 진
		선임연구원	이 재 익
		선임연구원	이 근 영
		연 구 원	최 지 선
		연 구 원	김 태 희
	침해대응지원팀	팀 장	민 상 식
자문 위원장	충남대학교	교 수	류 재 철
자문 위원	순천향대학교	교 수	곽 진
	강원대학교	교 수	김 상 춘
	카이스트	교 수	김 용 대
	서울여자대학교	교 수	김 윤 정
	고려대학교	교 수	김 휘 강
	정보통신기술진흥센터	정보보호CP	원 유 재
	숭실대학교	교 수	정 수 환
	한국인터넷진흥원	단 장	정 현 철

스마트폰 전자금융서비스 보안 가이드

발 행	2014년 7월
발행인	김 영 린
발행처	금융보안연구원
주 소	서울특별시 영등포구 의사당대로 143 금융투자협회 빌딩 8, 9F

<비 매 품>

본 가이드 내용의 무단전재를 금하며, 가공 인용할 때에는 반드시 금융보안연구원 『스마트폰 전자금융서비스 보안 가이드』라고 밝혀주시기 바랍니다.