발간등록번호
11-1312000-000057-01

2021. 10

모바일 전자정부 앱 검증 신청기관을 위한

모바일 전자정부서비스 앱 소스코드 검증 가이드라인

행정안전부
KISA 한국인터넷진흥원

발간등록번호
11-1312000-000057-01

2021. 10.

모바일 전자정부 앱 검증 신청기관을 위한

모바일 전자정부서비스 앱 소스코드 검증 가이드라인

행정안전부
KISA 한국인터넷진흥원

모바일 전자정부 앱 검증 신청기관을 위한

모바일 전자정부서비스 앱 소스코드 검증 가이드라인

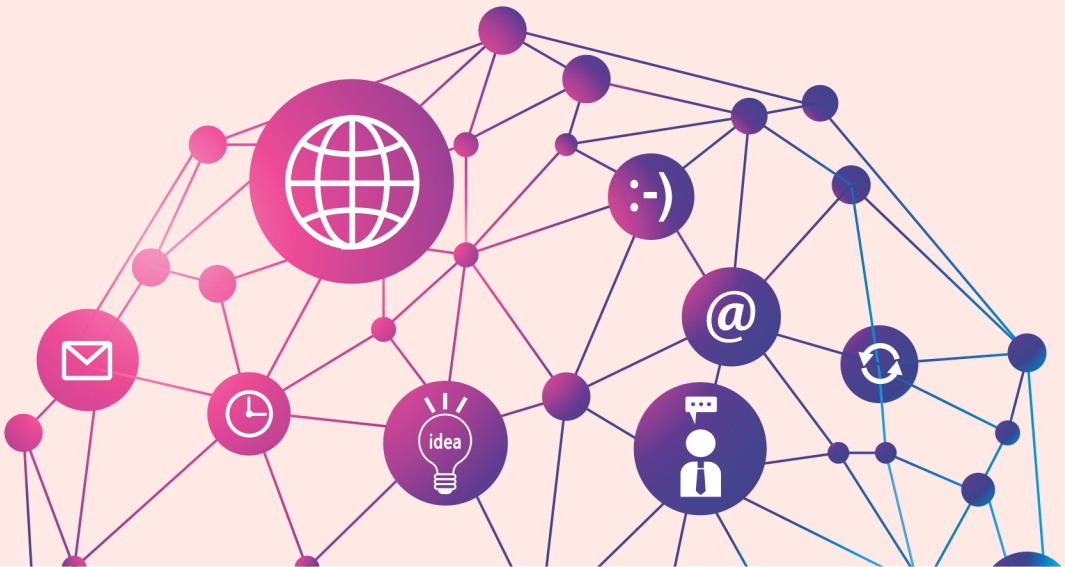
제·개정이력 Revision History

순번	제·개정일	변경내용	발간팀
1	2011.08.	**[제정]** • 모바일 앱 보안성 검증 안내서	공공소프트웨어보호팀
2	2012.08.	**[개정]** • 모바일 전자정부 지원센터 개소로 연계 검증에 따른 검증기준 및 절차 변경	공공소프트웨어보호팀
3	2013.09.	**[개정]** • 가이드라인으로 제목 변경 • 정보시스템 구축·운영지침의 소프트웨어 보안약점 기준 개정에 따라 소스코드 검증기준 변경 • 모바일 대국민 보안공통기반 구축·운영에 따른 기능 보안취약점 검증기준 추가	보안평가팀
4	2014.02.	**[개정]** • 모바일 전자정부 서비스 관리 지침 개정에 따른 검증절차 변경	보안평가팀
5	2015.12.	**[개정]** • 전자정부 소프트웨어·IoT 보안센터 개소에 따른 역할 명시 • 모바일 대민서비스 개발·운영시 고려사항 추가 • 모바일 전자정부 서비스 관리 지침의 개정에 따른 검증기준 등 추가	보안평가인증팀
6	2021.10.	**[개정]** • 기관 이전 및 명칭, 관련 규정 최신화	전자정부보호팀

목 차

Contents

[Part 1]
개 요



Part 1

개 요

『모바일 전자정부서비스 앱 소스코드 검증 체계』는 행정기관[1] 및 공공기관[2]에서 개발한 모바일 전자정부서비스 앱에 대해 소스코드 수준의 보안약점[3]을 사전 진단·제거하여 사용자들이 안심하고 모바일 전자정부 서비스를 사용할 수 있도록 지원하는 제도이다.

제 1 절 목적

- 본 가이드라인은 행정기관 및 공공기관 등에서 모바일 전자정부서비스 앱을 개발하여 전문기관(한국인터넷진흥원)으로 소스코드 검증을 신청할 때 참고하기 위한 검증 절차 및 기준 등에 대하여 소개하고자 한다.
  - 이를 통해 소스코드(Source Code) 수준의 소프트웨어(SW, Software) 보안약점이 제거된 모바일 전자정부서비스 앱을 보급함으로써 모바일 전자정부서비스의 안전성 및 신뢰성을 제고하고자 한다.
    ※ 모바일 전자정부서비스 구축 및 운영 시 고려사항은 행정안전부에서 발행한 『모바일 전자정부 서비스 구축 가이드라인』 참조
    ※ 모바일 전자정부서비스 앱 등록 관련은 행정안전부에서 발행한 『모바일 전자정부 공통기반 활용 가이드라인』 참조

1) 행정기관은 「전자정부법」 제2조 제2호에 따른 행정기관을 말한다.
2) 공공기관은 「전자정부법」 제2조 제3호에 따른 공공기관을 말한다.
3) 보안약점은 모바일 앱의 소프트웨어 결함, 오류 등으로 중요정보(개인정보, 위치정보, 업무정보 등) 유출, 해킹 등 사이버 공격을 유발할 가능성이 있는 잠재적인 보안취약점을 말함

제 2 절 적용범위

- 모바일 전자정부서비스는 사용대상에 따라 행정용과 대민용으로, 개발방식에 따라 모바일 웹, 반응형 웹, 모바일 앱, 하이브리드 앱(앱+웹)으로 구분된다.
- 본 가이드라인의 적용을 받는 소스코드 검증 대상은 신규(기능개선 포함)로 개발되는 모바일 전자정부서비스 중 모바일 앱과 하이브리드 앱으로만 한정된다.

적용범위

- 대상기관 : 행정기관, 공공기관 등
- 적용대상 : 신규(기능개선 포함)로 개발되는 모바일 앱, 하이브리드 앱
  ※ 검증 신청기관 요청 시 또는 전문기관 필요 시 모바일 앱(웹) 서버도 점검할 수 있음
  ※ 기능개선이 아닌 단순 컨텐츠(텍스트, 이미지 등) 변경은 소스코드 검증 대상이 아님

제 3 절 지침 및 가이드라인

- 모바일 전자정부서비스 앱 개발 또는 소스코드 보안약점 검증 관련 지침 및 가이드라인은 다음을 참고하면 된다.

  - 지침
    - 모바일 전자정부 서비스 관리 지침
    - 전자정부서비스 호환성 준수지침
    - 장애인·고령자 등의 정보 접근 및 이용 편의 증진을 위한 고시
    - 행정기관 및 공공기관 정보시스템 구축·운영 지침
    - 행정기관 도메인 이름 및 IP주소체계 표준
    - 모바일 전자정부 사용자 인터페이스 설계 지침
    - 전자정부 웹사이트 품질관리 지침

  - 가이드라인
    - 모바일 전자정부 서비스 구축 가이드라인
    - 모바일 전자정부 공통기반 활용 가이드라인

- 전자정부 모바일 표준프레임워크
- 대민 모바일 보안공통기반 활용 가이드라인
- 모바일 활용업무에 대한 보안 가이드라인
- 모바일 대민서비스 보안취약점 점검 가이드
- 모바일 전자정부 서비스 앱 소스코드 검증가이드라인
- 스마트폰 앱 접근권한 개인정보보호안내서
- 소프트웨어 개발보안 가이드
- 소프트웨어 보안약점 진단 가이드

제 4 절 모바일 대민서비스 개발·운영 시 고려사항

● 모바일 대민서비스(앱/웹)를 개발 또는 운영 시 고려사항은 다음과 같다.

- 모바일 대민서비스는 반응형 웹을 기본으로 개발
  - 단말 특성을 활용하거나 데이터 관리 등 서비스 특성으로 인해 웹으로 구축이 어려운 경우에는 앱으로 개발

    ※ 전화, SMS 등 모바일 기기의 특정 기능을 사용, 단말 내 중요정보 암호화 등 데이터 보호 기능 제공, 웹 브라우저에서 지원하지 않는 기능 제공

[모바일 앱으로 구현되어야 하는 기술(예시)]

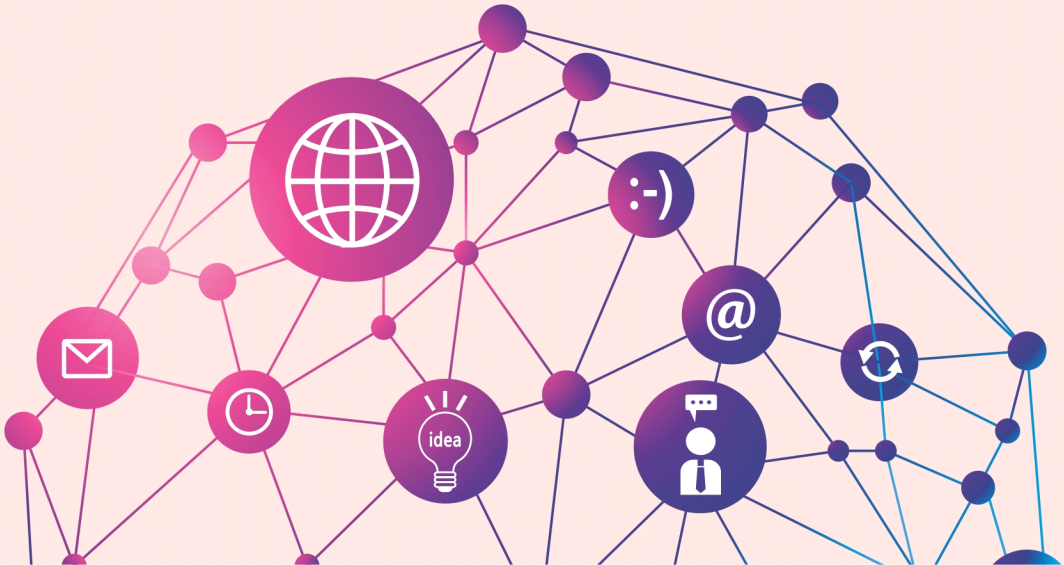
- 보편성 확보를 위해 '장애인·고령자 등의 정보 접근 및 이용 편의 증진을 위한 고시' 등 준수
- 앱 개발 시, SW개발보안을 적용하며 주요 항목은 모바일 전자정부 서비스 관리지침 등 참조
  - 운영 중에도 정기적으로 보안취약점을 자체적으로 점검·조치
  - 적용 범위 : 모바일 앱과 서비스 제공 서버 등
  - 관련 지침 : 「모바일 전자정부 서비스 관리 지침」 제4장, 모바일 전자정부 서비스 구축 가이드라인, 모바일 대민서비스 보안취약점 점검 가이드 등
- 모바일 앱 또는 하이브리드 앱은 행정기관등의 명의로 앱스토어에 등록·배포
  - 기능 검증을 실시하는 이동통신사 또는 제조사 등의 앱스토어를 반드시 1곳 이상 포함하여 등록

[Part 2]

모바일 전자정부서비스 앱 소스코드 검증체계

제1절 역할 및 책임

제2절 검증절차



Part 2

모바일 전자정부서비스 앱 소스코드 검증체계

『모바일 전자정부서비스 앱 소스코드 검증 체계』는 역할과 책임에 따라 정책기관, 검증기관, 신청기관으로 구분되며, 정책기관은 행정안전부, 전문기관은 한국인터넷진흥원으로 각 기관이 그 역할을 담당하고 있다.

제 1 절 역할 및 책임

● 모바일 전자정부서비스 앱 소스코드 검증과 관련하여 정책기관, 검증기관의 역할과 책임은 다음과 같다.

- 정책기관(행정안전부)
  - 모바일 전자정부서비스 앱 소스코드 검증 관련 제도 마련 및 정책 수립
  - 모바일 전자정부서비스 앱 소스코드 검증 관련 지침 및 가이드 배포
  - 모바일 전자정부서비스 앱 소스코드 검증 관련 기준 준수 권고
  - 모바일 전자정부서비스 지원을 위한 모바일 대국민 보안공통기반[4] 운영

- 전문기관(한국인터넷진흥원 전자정부 소프트웨어·IoT 보안센터)
  - 모바일 전자정부서비스 앱 소스코드 보안약점 진단
  - 모바일 전자정부서비스 앱 소스코드 진단기준 및 가이드 개발

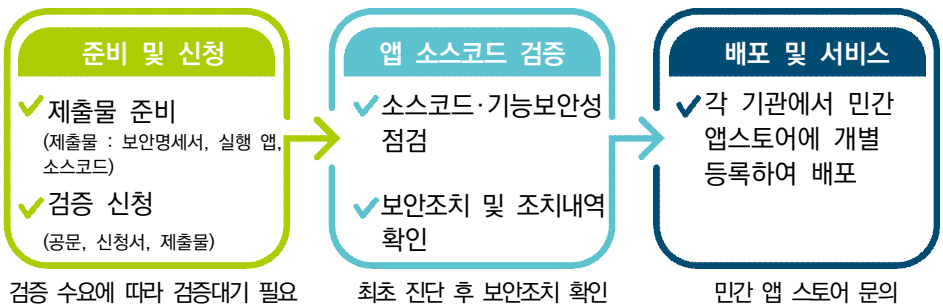
4) 국가기관 등이 모바일 서비스 구축 시 사용자 인증, 앱 위·변조 방지, 문서위변조 방지 등 공통적으로 적용할 수 있는 보안요소를 공동으로 활용할 수 있도록 제공하고자 하는 모바일 공용 프레임워크

[전자정부 소프트웨어·IoT 보안센터 시설 개요]	
구분	**시설 개요**
시설명	전자정부 소프트웨어·IoT 보안센터
위치	한국인터넷진흥원 나주 본원 2층 소재
연락처	☎ 061-820-2748, ✉ kisaappverify@kisa.or.kr

[전자정부 소프트웨어·IoT 보안센터 주요 역할]	
구분	**주요 역할**
보안성 검증	• 모바일 전자정부 서비스 앱의 소스코드 보안약점 진단 등 보안성 검증 – 취약점 조치 지원 및 제거 여부 점검 ※ 행정용 앱도 소스코드 검증을 신청할 경우 검증 가능
기술 지원	• 모바일 전자정부 대상 SW개발보안 적용 등 관련 기술 상시지원 – 모바일 서비스 암호화 등 관련 보안기능 적용 기술지원
기술 연구/ 교육·홍보	• 모바일 소프트웨어 보안 공격 동향, 신규 취약점 및 기술 연구 • 모바일 소프트웨어 보안 교육 및 홍보 등

제 2 절 검증 절차

● 본 가이드라인은 모바일 전자정부서비스 앱 소스코드 검증을 위한 절차 및 검증 기준을 기술하고 있으며, 검증단계는 다음과 같다.



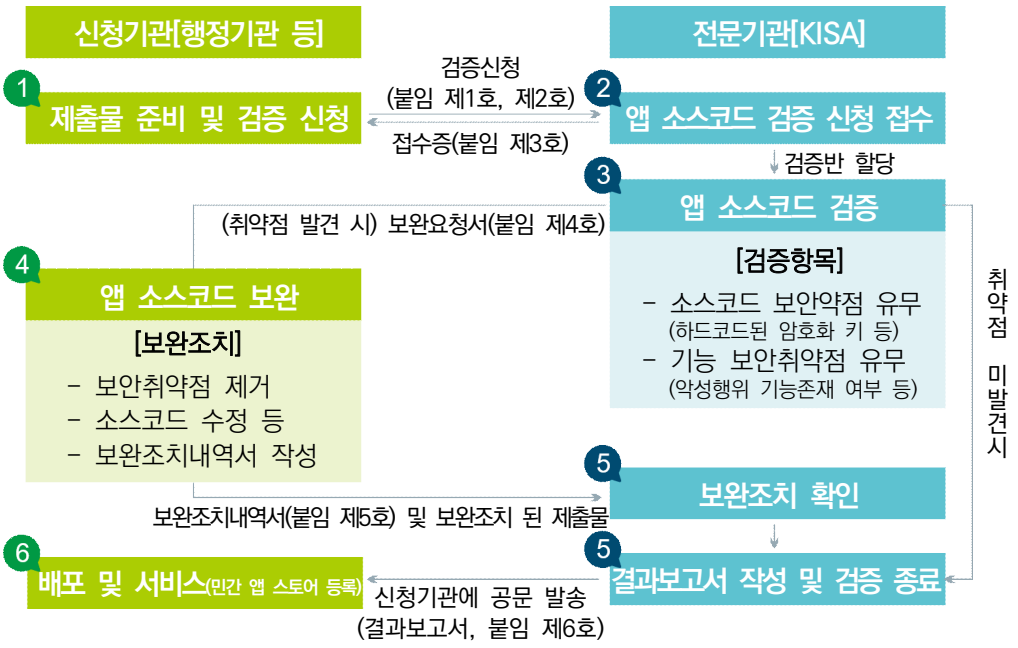
[모바일 전자정부서비스 앱 소스코드 검증단계]

- **준비 및 신청 단계**
  - 신청기관은 제출물을 준비한 후 전문기관에 온라인(전자공문)으로 소스코드 검증을 신청하며, 관련 제출물은 오프라인(방문제출 또는 등기우편)으로 제출한다.
  - 전문기관은 제출물 일체가 제출되면 접수번호가 표기된 접수증(붙임 제3호 서식)을 온라인형태로 신청기관에 발급한다.

제 출 물 (참고)

1) 검증신청 공문 및 검증신청서 (붙임 제1호 서식)
   ※ 전자문서를 통한 온라인 제출이 원칙이나, 전자공문이 지원되지 않는 기관의 경우 이메일(kisaappverify@kisa.or.kr)로 제출 가능
2) 신청제품의 컴파일 가능한 앱 소스코드 일체 및 실행파일(.apk, .ipa, .app, .cap 등)
   ※ 신청대상의 소스코드, 실행파일, 보안명세서 등 제출물은 CD(또는 DVD) 매체를 이용하여 방문 제출이 원칙이나, 방문 제출이 어려울 경우 등기우편을 이용하여 제출 가능
   (제출처) 전라남도 나주시 진흥길 9 한국인터넷진흥원 전자정부보호팀(우:58324)
   ※ 애플 iOS 기반 앱의 소스코드 제출 시, 해당 앱 개발환경인 애플 PC에서 압축파일 제작
3) 보안명세서 (붙임 제2호 서식)
   ※ 보안명세서는 신청대상의 식별정보(서비스명, 버전, 예상 배포 앱스토어 등) 및 보안 속성(필요 권한, 중요정보 등), 구현기능(기능 동작 설명 등)을 포함

- **앱 소스코드 검증 단계**
  - 전문기관은 신청된 모바일 서비스(이하 “검증 대상”)이 검증기준(제3장)에 명시된 소스코드 보안약점(하드코드된 비밀번호 등)과 기능 보안취약점(악성행위 기능 존재 여부 등)의 요구수준을 만족하는지 검증한다.
  - 검증대상에 대하여 보완이 필요할 경우 전문기관은 신청기관에 보완요청서(붙임 제4호 서식)를 통해 보완을 요청할 수 있다.
  - 신청기관은 해당 보완사항을 조치하여 전문기관에 보완조치내역서(붙임 제5호 서식)와 함께 보완 조치된 제출물을 제출해야 하며, 보완 조치된 제출물은 4주 내로 보완하여 전문기관에 제출하는 것을 원칙으로 한다.
  - 전문기관은 신청제품이 검증기준에 명시된 요구수준을 만족할 시 소스코드 검증 결과보고서(붙임 제6호 서식)를 신청 기관에 통보한다.



[모바일 전자정부서비스 앱 소스코드 검증 세부 절차]

주요 FAQ

1) 모바일 전자정부서비스 앱 소스코드 검증 순서는 어떻게 되나요?
   → 검증신청 제품은 접수한 순서(접수번호)에 따라 검증 수행
2) 모바일 전자정부서비스 **앱 소스코드 검증(❸)**에 소요되는 전체 기간은?
   → 검증 착수 후 2주일. 단, 검증 대상의 기능 및 소스코드 양에 따라 차이 존재
   ※ 검증 대상에서 보안약점 도출 시 신청기관에서 보완·조치한 내역을 확인하기 위해 추가적인 기간이 소요될 수 있음
   ※ 검증 수요가 많을 시 검증 대기 기간이 발생하여, 검증 기간이 길어질 수 있음
3) **보완요청 발생 시** 어떻게 해야 하나요?
   → 보완조치내역서(붙임 제5호 서식)와 보완·조치된 제출물(소스코드 등)을 제출
4) **앱 소스코드 보완(❹)** 관련 제출기한이 정해져 있나요?
   → 신청기관은 **4주 이내**로 보완하여 전문기관(한국인터넷진흥원)에 다시 제출
   ※ 보완요청 이후 4주 경과 또는 동일한 사항으로 보완요청 2회 초과 시, 전문기관은 신청기관에 검증종료를 통보할 수 있음
5) **보완조치 확인(❺)**에 소요되는 기간은?
   → 앱 소스코드 검증(❸)에 소요되는 기간과 동일함

- **배포 및 서비스 단계**
  - 신청기관은 앱 소스코드 검증이 완료된 후에 해당 앱에 대한 배포 및 서비스 제공을 위해 민간 앱스토어 등을 통해 서비스 등록을 신청한다.
  - 한국인터넷진흥원을 통해 모바일 앱을 검증받은 경우에는 최종 수정사항을 확인받아 민간 앱스토어 등에 서비스를 배포한다.
  - 신청기관은 민간 앱스토어 등을 통해 등록·배포한 모바일 대민서비스 정보를 범정부 정보기술아키텍처 지원시스템(범정부EA포털)에 등록한다.

주요 FAQ

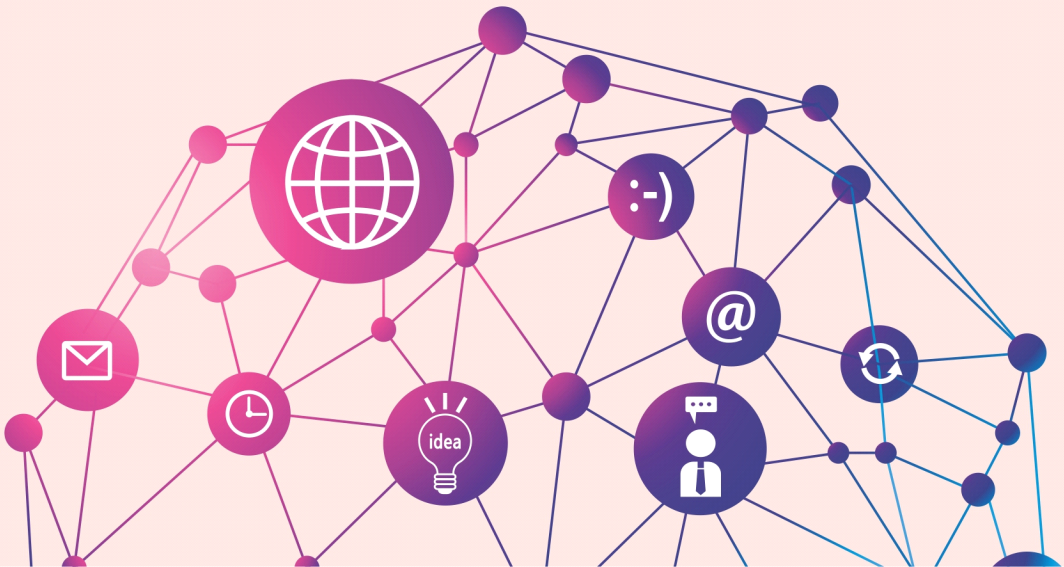
1) 모바일 전자정부서비스 앱에 대한 등록신청은 어떻게 하나요?
   → 모바일 대민서비스 앱의 경우에는 민간 앱스토어를 반드시 1곳 이상 포함하여 등록하며, 앱스토어 등록 시 해당 행정기관등의 명의로 등록
   ※ 자세한 사항은 『모바일 전자정부서비스 구축 가이드라인』을 참조
   → 행정(내부망)망을 이용하여 http://www.mobile.go.kr 사이트에 On-Line 등록
   ※ 자세한 사항은 『모바일 전자정부 공통기반 및 지원센터 활용 가이드라인』을 참조
2) 모바일 전자정부서비스 앱에 대한 배포 방법은 어떻게 되나요?
   → "모바일 업무포털" 등 행정용 앱은 지원센터에서 운영하는 행정용 앱스토어를 통해 배포
   → "정부24" 등 대민용 앱은 국내 이동통신사 또는 제조사 등의 민간 앱스토어를 통해 신청기관이 직접 배포
3) 범정부 정보기술아키텍처 지원시스템(범정부EA포털)은 무엇인가요?
   → "범정부 정보기술아키텍처 지원시스템"은 정보기술아키텍처 관련 정보를 공동으로 등록·관리·활용할 수 있도록 구축·운영하는 시스템
   ※ 자세한 사항은 범정부EA포털(https://geap.go.kr) 사이트를 참조

[Part 3]

모바일 전자정부서비스 앱 소스코드 검증기준

제1절 소스코드 보안약점
(Source Code Weakness)

제2절 기능 보안취약점
(Function Vulnerability)



Part 3

모바일 전자정부서비스 앱 소스코드 검증 기준

『모바일 전자정부서비스 앱 소스코드 검증 기준』은 앱 제공 기능상에 내포될 수 있는 기능 보안취약점 및 『모바일 전자정부 서비스 관리 지침』에 따른 소스코드 보안약점 등으로 구성된다.

제 1 절 소스코드 보안약점(Source Code Weakness)

● 모바일 전자정부서비스 앱은 개발과정에서 다음의 소스코드 검증기준을 만족하여야 한다.

※ 행정기관등의 장은 『모바일 전자정부 서비스 관리 지침(행정안전부예규)』의 '모바일 앱 보안약점' 점검기준 26개 항목(별표 3) 및 모바일 대민서비스 보안취약점 점검가이드[5] 등을 준수하여 구현언어 기반의 소스코드 보안약점을 진단하고 제거하여야 한다.

- **입력데이터 검증 및 표현(5개 항목)**
  - 프로그램 입력 값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식 지정으로 인해 발생할 수 있는 보안약점을 제거하여야 한다.

세부 보안 약점

1	SQL 삽입	4	운영체제 명령어 삽입
2	경로 조작 및 자원 삽입	5	오버플로우(정수형, 메모리 버퍼)
3	크로스사이트 스크립트	-	

5) 행정안전부, "모바일 전자정부 대민서비스 개발자를 위한 모바일 대민서비스 보안취약점 점검 가이드"

- **보안기능(8개 항목)**
  - 보안기능(인증, 기밀성, 암호화 등)을 부적절하게 구현 시 발생할 수 있는 보안약점을 제거하여야 한다.

세부 보안 약점

1	취약한 암호화 알고리즘 사용	5	충분하지 않은 키 길이 사용
2	중요정보 평문 저장	6	적절하지 않은 난수값 사용
3	중요정보 평문 전송	7	하드코드된 암호화 키
4	하드코드된 비밀번호	8	주석문안에 포함된 시스템 주요정보

- **시간 및 상태(1개 항목)**
  - 동시 또는 거의 동시 수행을 지원하는 병렬 시스템, 하나 이상의 프로세스가 동작되는 환경에서 시간 및 상태를 부적절하게 관리하여 발생할 수 있는 보안약점을 제거하여야 한다.

세부 보안 약점

1	경쟁조건 : 검사 시점과 사용 시점(TOCTOU)

- **에러처리(3개 항목)**
  - 에러를 처리하지 않거나, 불충분하게 처리하여 에러 정보에 중요정보(시스템 등)가 포함될 때 발생할 수 있는 보안약점을 제거하여야 한다.

세부 보안 약점

1	오류 메시지 및 시스템 데이터 정보노출	3	부적절한 예외 처리
2	오류 상황 대응 부재	-	

- **코드오류(2개 항목)**
  - 자원(메모리 등)의 부적절한 반환 등과 같이 개발자가 범할 수 있는 코딩오류로 인해 유발되는 보안약점을 제거하여야 한다.

세부 보안 약점

1	Null Pointer 역참조	2	부적절한 자원 해제

• **API 오용(1개 항목)**

- 의도된 사용에 반하는 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안약점을 제거하여야 한다.

세부 보안 약점

1	취약한 API 사용

• **모바일 환경 특화(6개 항목)**

- 공개영역(CWE[6], CWE/SANS Top25[7], OWASP Mobile Top 10[8] 등) 등을 통해 모바일 환경에 특화된 보안약점이 발견되지 않도록 제거하여야 한다.

세부 보안 약점

1	안드로이드 애플리케이션 컴포넌트의 부적절한 접근 허용	4	안드로이드 권한 검사 우회
2	민감한 정보 전송을 위한 암시적 intent 사용	5	클래스 로딩 하이재킹
3	접근제어 없이 내·외부 저장소 사용	6	소스코드 난독화 미적용

6) CWE(Common Weakness Enumeration), http://cwe.mitre.org

7) CWE/SANS Top25 Most Dangerous Software Errors, http://www.sans.org

8) OWASP(Open Web Application Security Project) Mobile Top 10, https://www.owasp.org

제 2 절 기능 보안취약점(Function Vulnerability)

● 모바일 전자정부서비스 앱은 기능에 대한 다음의 보안취약점 검증기준을 만족하여야 한다.

※ 행정기관등의 장은 『모바일 전자정부 서비스 관리 지침(행정안전부예규)』에 따라 모바일 앱에 대해 정기적으로 보안취약점을 점검해야 하며, 이때 '모바일 앱 보안취약점' 점검기준 20개 항목(별표 1)을 필수 점검항목으로 포함하여야 한다.

• 임의기능 존재 여부

- 기능설명(보안명세서, UI명 등) 내용과 실제 앱 기능이 일치해야 한다.

세부 점검 항목

- 명세되지 않은 기능 존재 여부
- 악성행위(불법 녹음, 임의 데이터 전송, 임의로 위치정보 수집 등) 기능 존재 여부

• 최소 권한

- 기능 동작에 필요한 최소 권한만 부여 되어야 한다.

세부 점검 항목

- (공통) 관리자 권한으로 동작되는 기능 존재 여부(권한상승 등 포함)
- (공통) 인가되지 않은 API 사용
- (Android) 동일한 개인키로 서명된 다른 앱과 UID 공유 여부
- (Android) 기능사용 요청 권한과 기능사용 여부 적절성 여부
- (Android) 인텐트 권한의 올바른 설정 여부

• 입력값 유효성

- 외부 입력정보를 기반으로 기능 동작 시, 입력정보에 대한 유효성을 검증해야 한다.

세부 점검 항목

- 외부 입력 값의 유효성(예, 지정된 길이 초과, 악성코드 포함 등) 검증 기능 존재 여부

• 중요정보 관리

– 중요정보(개인정보, 사용자 인증 및 계정정보, 개인위치정보 등)는 안전하게 관리(저장, 전송 등)되어야 한다.

세부 점검 항목 (인증정보)

- 사용자 인증 및 계정관리 보안 요구사항
  - 민원인의 경우, 아이디와 비밀번호를 사용하고 신분증명이 필요한 경우 공동인증서 사용
  - 비밀번호 조합규칙(영문·숫자·특수문자 등 조합하여 8자리 이상 등)
    ※ 한국인터넷진흥원, 패스워드 선택 및 이용 안내서 참고

세부 점검 항목 (위치정보)

- 위치정보 저장·전송 등 보안 요구사항
  - 개인 위치정보의 안전한 저장 및 전송을 위한 암호화 적용 여부
    ※ 위치정보의 관리적·기술적 보호조치 권고 제 8조(위치정보시스템의 권한 없는 접근을 차단하기 위한 암호화·방화벽 설치 등의 조치)

세부 점검 항목 (개인정보)

- 개인정보 저장·전송 등 보안 요구사항
  - 주민등록번호, 여권번호, 면허번호, 외국인등록번호, 금융정보(계좌정보 등)에 대한 암호화 저장 및 전송 여부
  - 비밀번호 및 바이오정보에 대한 일방향 암호화 저장 여부
    ※ 개인정보보호법 제24조(고유식별정보의 처리 제한) 제3항

주요 FAQ

[개인정보 관련 참고사항]

- (참고) 개인정보 수집 시, 법에서 언급한 불가피한 경우를 제외하고 정보주체의

동의를 받아야 하며, 수집·이용 목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용기간 등을 알려야 함

※ 개인정보 보호법 제15조(개인정보의 수집·이용)

- (참고) 개인정보 불필요 시(보유기간 경과, 처리목적 달성 등) 복구·재생되지 않도록 파기

※ 개인정보 보호법 제21조(개인정보의 파기)

[위치정보 관련 참고사항]

- (참고) 개인위치정보 수집 시, 긴급구조기관의 긴급구조 등을 제외하고 위치정보주체 동의를 받아야 하며, 위치정보사업자의 상호 및 연락처, 위치정보 수집사실 확인 자료의 보유근거 및 보유기간 등을 이용약관에 명시하여야 함

※ 위치정보의 보호 및 이용 등에 관한 법률 제18조(개인위치정보의 수집)

- (참고) 개인위치정보의 수집, 이용 또는 제공목적 달성 시, 개인위치정보는 즉시 파기해야 함

※ 위치정보의 보호 및 이용 등에 관한 법률 제23조(개인정보의 파기 등)

• 플랫폼 보안 모델

– 구현기능은 모바일 플랫폼의 보안모델에 위배되지 않아야 한다.

세부 점검 항목

- 루팅, 탈옥 등과 같은 플랫폼 변조 기능 존재 여부
- 플랫폼에서 제공하는 보안기능 사용의 적절성 여부

• 상용/공개용 모듈

– 상용 또는 공개모듈(소스코드 미제공)을 사용하여 기능 구현 시, 해당 모듈에 대한 안전성은 보증되어야 한다.

세부 점검 항목

- 상용 또는 공개모듈 사용 목적 및 기능의 적절성 여부
- 해당 모듈에 대한 개발업체의 안전성 확인 방법 및 결과의 적절성 여부

- **공개영역 취약점**
  - 공개영역(웹 사이트 등) 등을 통해 잘 알려진 취약점이 발견되지 않아야 한다.

세부 점검 항목

- 모바일 플랫폼(안드로이드, iOS, 윈도우모바일 등) 등에 대해 알려진(및 신규) 취약점 존재 여부

- **모바일 대국민서비스 보안공통기반 적용여부 및 제공 기능에 대한 검증**
  - 모바일 대국민 보안공통기반을 적용한 앱의 경우 해당 기능 적용에 따른 보안 취약점이 발견되지 않아야 한다.
  - 보안공통기반을 적용하지 않은 앱의 경우에는 공통기반에서 제공하는 기능에 부합되도록 보안이 제공되어야 한다.(앱 위·변조 등)

- **기타**
  - 위 항목(임의기능 존재 여부 등)외 검증대상 제품에 특화된 보안취약점이 발견되지 않아야 한다.
  - 모바일 앱에 대한 역공학 공격을 방어하기 위해 모바일 앱 개발시 코드 난독화 도구(또는 옵션)을 적용하는 것이 필요하다.

앱위변조 (참고)

[앱 위·변조 관련 참고사항]

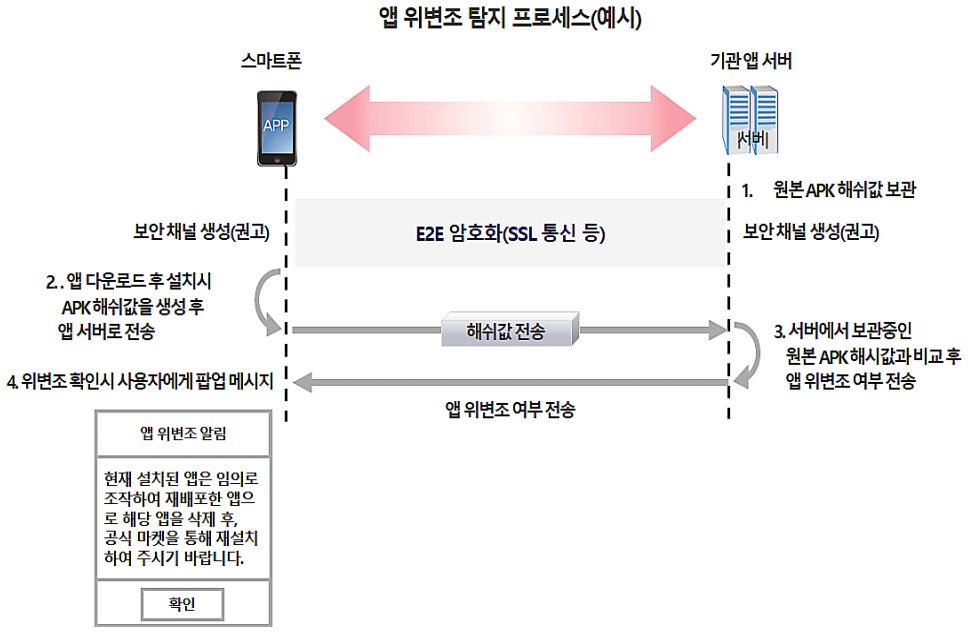
- 안드로이드 플랫폼 기반의 모바일 앱의 경우, 해커에 의해 위·변조된 앱을 다운로드·설치 시 중요정보 탈취 등 보안사고가 발생할 수 있으므로, 앱 설치 시 앱 위·변조 여부 확인 필요

[앱 위·변조 관련 적용 방법]

- 모바일 앱 위·변조를 탐지할 수 있는 상용 솔루션을 도입하거나, 기관 자체적으로 최소한의 위·변조 탐지 기능을 구현

[(구현예시) 앱 설치시 앱 위변조 탐지 기능]

1. (기관) 서비스 제공 앱 서버
   - 앱 배포 전 실행파일(.apk)에 대한 해쉬값[9]을 생성하여 보관(①)
   - 사용자 단말기에서 전송된 해쉬값과 서버에 보관된 해쉬값을 비교하여 위·변조 여부 전송(③)
2. (사용자) 모바일 앱
   - 앱 설치 시 앱 실행파일(.apk)에 대한 해쉬값을 생성하여 앱 서버로 전송(②)
   - 앱 서버에서 전송된 정보를 기반으로 위·변조 확인 시 사용자에게 팝업 메시지를 보여주어 위·변조 앱 설치 중지 및 삭제 유도(④)
3. (통신) 앱과 서버 간 통신은E2E 암호화(TLS 통신 등) 적용 권고



9) 안드로이드 해쉬 함수 : java.security.MessageDigest, http://docs.oracle.com/javase/6/docs/api/java/security/MessageDigest.html

난독화 적용 (참고)

[난독화 적용 관련 참고사항]

- 안드로이드 플랫폼 기반의 모바일 앱의 경우, 디컴파일 도구(예, apktool) 이용 시 실행파일(.apk)을 소스코드 원본 수준으로 쉽게 변환시킬 수 있으며, 이를 통해 앱 구조 및 소스코드 파악이 가능하고 위·변조 등에 활용될 수 있음. 이러한 위협을 예방하기 위해서는 난독화 도구 등을 적용하여 모바일 앱을 패키징하여야 함

[난독화 기술 적용 방법]

- 난독화 기능이 우수한 상용도구를 이용하는 것을 권고하나, 그러지 못할 경우 최소한 구글에서 제공하는 오픈소스 난독화도구(ProGuard[10]) 등을 적용
  ※ 다만, 오픈소스 난독화 도구는 상용도구 수준의 기능·보안성을 담보하지 않음

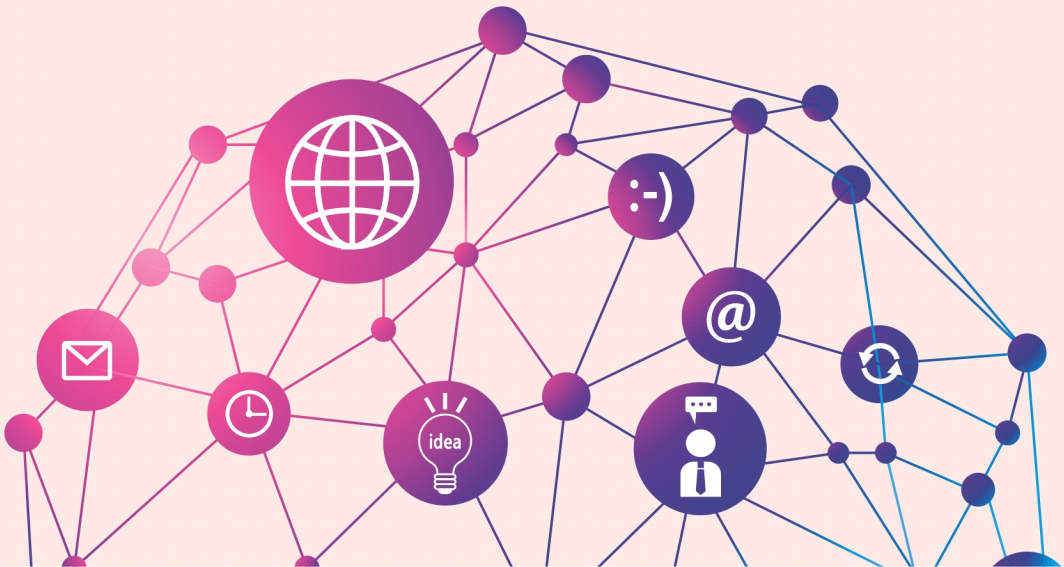
[오픈소스 난독화도구(ProGuard) 적용 방법]

1. Android Studio 내 main module 내에 있는 build.gradle에 설정 값 추가
2. build.gradle파일 내 minifyEnabled를 true로 설정

```
buildTypes {
        debug {
            minifyEnabled true
        }
        release {
            minifyEnabled true
            proguardFiles getDefaultProguardFile('proguard-android.txt'), 'proguard-rules.pro'
        }
    }
```

10) 구글 난독화 도구(ProGuard) : https://www.guardsquare.com/proguard

별표 및 서식



별표 제1호 소스코드 보안약점 검증기준 항목 설명

1. 입력데이터 검증 및 표현

번호	보안약점명	설 명
1	SQL 삽입	검증되지 않은 외부 입력값이 SQL 쿼리문 생성에 사용되어 악의적인 쿼리가 실행 될 수 있는 보안약점
2	경로조작 및 자원삽입	검증되지 않은 외부 입력값이 시스템 자원 접근경로 또는 자원제어에 사용되어 공격자가 입력값을 조작해 공격할 수 있는 보안약점
3	크로스사이트 스크립트	검증되지 않은 외부 입력값에 의해 사용자 브라우저에서 악의적인 스크립트가 실행될 수 있는 보안약점
4	운영체제 명령어 삽입	검증되지 않은 외부 입력값이 운영체제 명령어 생성에 사용되어 악의적인 명령어가 실행될 수 있는 보안약점
5	오버플로우 (정수형, 메모리 버퍼)	정수값 및 메모리 버퍼의 경계값이 범위를 넘어서는 경우, 프로그램이 예기치 않게 동작될 수 있는 보안약점

2. 보안기능

번호	보안약점명	설 명
1	취약한 암호화 알고리즘 사용	중요정보(비밀번호, 개인정보 등)의 기밀성을 보장할 수 없는 취약한 암호화 알고리즘을 사용하여 정보가 노출될 수 있는 보안약점
2	중요정보 평문저장	중요정보(비밀번호, 개인정보 등)을 암호화하여 저장하지 않아 정보가 노출될 수 있는 보안약점
3	중요정보 평문전송	중요정보(비밀번호, 개인정보 등) 전송시 암호화하지 않거나 안전한 통신채널을 이용하지 않아 정보가 노출될 수 있는 보안약점
4	하드코드된 비밀번호	소스코드내에 비밀번호가 하드코딩되어 소스코드 유출시 노출 우려 및 주기적인 변동 등 수정(관리자 변경 등)이 용이하지 않는 보안약점
5	충분하지 않은 키 길이 사용	데이터의 기밀성, 무결성 보장을 위해 사용되는 키의 길이가 충분하지 않아 기밀정보 누출, 무결성이 깨지는 보안약점
6	적절하지 않은 난수 값 사용	예측 가능한 난수사용으로 공격자로 하여금 다음 숫자 등을 예상하여 시스템 공격이 가능한 보안약점
7	하드코드된 암호화 키	소스코드내에 암호화키가 하드코딩되어 소스코드 유출시 노출 우려 및 키 변경이 용이하지 않는 보안약점
8	주석문 안에 포함된 시스템 주요정보	소스코드내의 주석문에 인증정보 등 시스템 주요정보가 포함되어 소스코드 유출시 노출될 수 있는 보안약점

3. 시간 및 상태

번호	보안약점명	설 명
1	경쟁조건 : 검사 시점과 사용 시점(TOCTOU)	멀티 프로세스 상에서 자원을 검사하는 시점과 사용하는 시점이 달라서 발생하는 보안약점

4. 에러처리

번호	보안약점명	설 명
1	오류메시지 및 시스템 데이터 정보노출	사용자가 볼 수 있는 오류 메시지나 스택 정보에 시스템 내부 데이터나 디버깅 관련 정보가 공개되는 보안약점
2	오류상황 대응 부재	시스템에서 발생하는 오류상황을 처리하지 않아 프로그램 실행정지 등 의도하지 않은 상황이 발생할 수 있는 보안약점
3	부적절한 예외 처리	예외에 대한 부적절한 처리로 인해 의도하지 않은 상황이 발생될 수 있는 보안약점

5. 코드오류

번호	보안약점명	설 명
1	Null Pointer 역참조	Null로 선언된 객체의 주소값을 참조했을 때 발생하는 보안약점
2	부적절한 자원 해제	사용된 자원을 적절히 해제하지 않으면 자원 누수 등이 발생하고, 자원이 부족하여 새로운 입력을 처리할 수 없게 되는 보안약점

6. API 오용

번호	보안약점명	설 명
1	취약한 API 사용	취약하다고 알려진 함수를 사용함으로써 예기치 않은 보안위협에 노출될 수 있는 보안약점

7. 모바일 환경 특화

번호	보안약점명	설 명
1	안드로이드 애플리케이션 컴포넌트의 부적절한 접근 허용	안드로이드 애플리케이션 컴포넌트 설정으로 부적절한 접근이 허용되어 외부의 애플리케이션에 의해 의도치 않게 실행될 수 있는 보안약점
2	민감한 정보 전송을 위한 암시적 intent 사용	암시적 intent를 사용하여 민감한 정보가 전송시 도청 및 악성행위 삽입이 가능한 보안약점
3	접근제어 없이 내·외부저장소 사용	내·외부저장소(SD카드 등)에 중요한 정보를 암호화하여 저장하지 않아 정보가 노출되거나 수정이 가능한 보안약점
4	안드로이드의 권한 검사 우회	권한이 전혀 없는 호출 프로그램이 응용 프로그램의 권한을 사용하게 되어 권한 검사를 우회할 수 있는 보안약점
5	클래스 로딩 하이재킹	프로그램의 클래스 로드시 검색되는 디렉토리의 이름이 변경되어 클래스 경로를 공격자가 명시적으로 제어할 수 있는 보안약점
6	소스코드 난독화 미적용	역공학 기술에 의한 소스코드 유출 및 보안메커니즘 우회 등이 발생할 수 있는 보안약점

별표 제2호 기능 보안취약점 검증기준 항목 설명

항목		세부 점검내용	
FV-1	임의기능	FV-1.1	명세 되지 않은 기능 존재 여부
		FV-1.2	악성행위 기능 존재 여부 (불법 녹음, 임의 데이터 전송, 임의로 위치정보 수집·전송 등)
FV-2	최소권한	FV-2.1	관리자 권한으로 동작되는 기능(권한상승 포함) 존재 여부(공통)
		FV-2.2	인가되지 않은 API 사용(공통)
		FV-2.3	동일한 개인키로 서명된 다른 앱과 UID 공유 여부(Android)
		FV-2.4	기능 사용 요청 권한과 기능 사용 여부 적절성 여부(Android)
		FV-2.5	인텐트 권한의 올바른 설정 여부(Android)
FV-3	입력값 유효성	FV-3.1	외부 입력값의 유효성 (지정된 길이 초과, 악성코드 포함 등) 검증 기능 존재 여부
FV-4	중요정보 관리	FV-4.1	개인정보의 안전한 저장 및 전송을 위한 암호화 적용 여부 (주민등록번호, 여권번호, 면허번호, 외국인등록번호, 금융정보 등)
		FV-4.2	비밀번호 및 바이오정보에 대한 일방향 암호화 저장 여부
		FV-4.3	개인위치정보의 안전한 저장 및 전송을 위한 암호화 적용 여부
		FV-4.4	기타 중요정보의 안전한 저장 및 전송을 위한 암호화 적용 여부
		FV-4.5	개인정보 및 위치정보 수집 및 활용에 대한 동의 여부
		FV-4.6	사용자 인증 방법의 적절성 유무
		FV-4.7	비밀번호 조합규칙(영문·숫자·특수문자 등 조합 9자리 이상 등)
		FV-4.8	앱과 관련된 앱(또는 웹) 서버의 기능, 중요정보 관리기능 등 점검
FV-5	플랫폼 보안모델	FV-5.1	루팅, 탈옥 등과 같은 플랫폼 변조 기능 존재 여부
		FV-5.2	플랫폼에서 제공하는 보안기능 사용의 적절성 여부
FV-6	상용/공개용 모듈	FV-6.1	상용 또는 공개모듈 사용 목적 및 기능의 적절성 여부
		FV-6.2	해당 모듈에 대한 개발사의 안전성 확인 방법, 결과의 적절성 여부
FV-7	공개영역 취약점	FV-7.1	모바일 플랫폼(예, 안드로이드, iOS, 윈도우모바일 등) 등에 대해 알려진(및 신규) 취약점 존재 여부
FV-8	모바일 대국민 보안공통기반 적용의 적절성	FV-8.1	모바일 공통기반 기능 구현의 적절성 여부
		FV-8.2	보안공통기반을 적용하지 않은 앱의 경우에는 공통기반에서 제공하는 기능에 부합되도록 보안이 제공
FV-9	기타	FV-9.1	신청제품의 서비스 특성에 따른 추가적인 보안취약점 존재 여부
		FV-9.2	모바일 앱 개발 및 배포 시 코드 난독화 도구 사용 여부

별표 제3호 기능 보안취약점 검증기준 항목 비교

기능 보안취약점 세부 점검내용		모바일 전자정부 서비스 관리 지침 내 모바일 앱 보안취약점 점검기준(별표1)	
FV-1.1	명세 되지 않은 기능 존재 여부	1	반복 설치 시 오류 발생
FV-1.1	명세 되지 않은 기능 존재 여부	2	앱 설치 전후 비정상적인 파일 및 디렉토리 설치
FV-2.4	기능 사용 요청 권한과 기능 사용 여부 적절성 여부(Android)	3	불필요하거나 과도한 권한 설정
FV-1.1	명세 되지 않은 기능 존재 여부	4	앱 삭제 후 안전성
FV-1.1	명세 되지 않은 기능 존재 여부	5	기능의 정상동작
FV-1.2	악성행위 기능 존재 여부(불법 녹음, 임의 데이터 전송, 임의로 위치정보 수집·전송 등)	6	임의기능 등 악성행위 기능 존재
FV-2.1	관리자 권한으로 동작되는 기능(권한상승 포함) 존재 여부(공통)		
FV-2.2	인가되지 않은 API 사용(공통)		
FV-3.1	외부 입력값의 유효성(지정된 길이 초과, 악성코드 포함 등) 검증 기능 존재 여부		
FV-4.8	앱과 관련된 앱(또는 웹) 서버의 기능, 중요정보 관리기능 등 점검(필요시 점검 수행)	7	정보 외부 유출
FV-1.2	악성행위 기능 존재 여부(불법 녹음, 임의 데이터 전송, 임의로 위치정보 수집·전송 등)	8	자원고갈
FV-5.1	루팅, 탈옥 등과 같은 플랫폼 변조 기능 존재 여부	9	루팅 및 탈옥 기기에서의 정상 동작
FV-2.1	관리자 권한으로 동작되는 기능(권한상승 포함) 존재 여부(공통)	10	ID 값의 변경
FV-2.3	동일한 개인키로 서명된 다른 앱과 UID 공유 여부(Android)	11	동일키로 서명된 서로 다른 앱 간의 UID 공유
FV-2.5	인텐트 권한의 올바른 설정 여부(Android)	12	인텐트 권한의 올바른 설정
FV-4.6	사용자 인증 방법의 적절성 유무	13	인증 정보 생성 강도 적절성
FV-4.7	비밀번호 조합규칙(영문·숫자·특수문자 등 조합 9자리 이상 등)		
FV-4.1	개인정보의 안전한 저장 및 전송을 위한 암호화 적용 여부 (주민등록번호, 여권번호, 면허번호, 외국인등록번호, 금융정보 등)	14	중요정보의 평문 저장 및 전송
FV-4.2	비밀번호 및 바이오정보에 대한 일방향 암호화 저장 여부		
FV-4.3	개인위치정보의 안전한 저장 및 전송을 위한 암호화 적용 여부		
FV-4.1	개인정보의 안전한 저장 및 전송을 위한 암호화 적용 여부 (주민등록번호, 여권번호, 면허번호, 외국인등록번호, 금융정보 등)	15	중요정보 저장 및 전송 시 취약한 암호알고리즘 적용
FV-4.2	비밀번호 및 바이오정보에 대한 일방향 암호화 저장 여부		
FV-4.3	개인위치정보의 안전한 저장 및 전송을 위한 암호화 적용 여부		
FV-4.4	기타 중요정보의 안전한 저장 및 전송을 위한 암호화 적용 여부	16	기타 중요 정보의 평문 저장 및 전송
FV-4.4	기타 중요정보의 안전한 저장 및 전송을 위한 암호화 적용 여부	17	기타 중요 정보 저장 및 전송 시 취약한 암호 알고리즘 적용
FV-4.8	앱과 관련된 앱(또는 웹) 서버의 기능, 중요정보 관리기능 등 점검(필요시 점검 수행)	18	파일 다운로드 시 외부주소 변조 및 파일 무결성 우회
FV-4.5	개인정보 및 위치정보 수집 및 활용에 대한 동의 여부	19	개인정보 및 개인위치정보 수집 및 활용에 대한 동의
FV-9.2	모바일 앱 개발 및 배포 시 코드 난독화 도구 사용 여부	20	난독화

붙임 제1호 서식 신청서

(앞 면)

접 수 번 호 제 호	모바일 전자정부서비스 앱 소스코드 검증 신청서			
신청기관	① 신청기관명			
	② 담당자(직책)		부서명	
			전화	
			이메일	
개발기관	③ 개발사명			
	④ 개발자(직책)		부서명	
			전화	
			이메일	
검증신청 대상정보	⑤ 서비스명			
	⑥ 서비스유형	☐모바일 대민서비스 ☐모바일 행정서비스 ☐기타( )		
	⑦ 구현유형	☐모바일 앱 ☐하이브리드 앱 ☐기타( )		
	⑧ 개발언어	☐Android-Java ☐Object-C ☐기타( )		
	⑨ 프레임워크	☐전자정부 프레임워크 ☐기타( )		
	⑩ 운영체제	☐Android( ) ☐iOS( ) ☐기타( )		
	⑪ 앱 식별자			
	⑫ 공통기반	☐사용( ) ☐사용안함		

상기와 같이 모바일 전자정부서비스 앱 소스코드 등에 대한 검증을 신청하며, 기재사항에 허위사실이 없음을 확인합니다.

년 월 일

신청기관 담당자 (서명 또는 인)

한국인터넷진흥원장 귀하

붙임 제1호 서식 **신청서**

(뒷 면)

모바일 전자정부서비스
앱 소스코드 검증 신청서 작성요령

1. 해당하는 빈칸에 ☑ 와 같이 표기한다.

2. 각 항목의 작성요령은 다음과 같다.

① 신청기관의 기관명을 기재한다.

② 검증신청 업무 담당자 성명, 직책, 부서명, 전화번호, 이메일주소 등을 기재한다.

③ 개발기관의 상호 또는 명칭을 기재한다.

④ 개발업무 담당자 성명, 직책, 부서명, 전화번호, 이메일주소 등을 기재한다.

⑤ 앱 서비스 명칭을 기재한다.

⑥ 앱 서비스 유형에 따라 해당 항목에 표기한다.

⑦ 앱 구현 유형에 따라 해당 항목에 표기한다.

⑧ 앱 개발언어를 표기한다.

⑨ 앱 프레임워크 유형에 따라 해당 항목에 표기한다.

⑩ 앱 설치운영 대상 운영체제 명칭과 버전번호를 표기한다.

⑪ 앱 식별자(예, kr.or.kisa.app)를 기재한다.

⑫ 모바일 대국민 보안공통기반 사용 여부 및 사용하는 기능을 표기한다.

모바일 전자정부서비스
앱 소스코드 검증 보안명세서

〈 검증대상 제품명 〉

년 월 일

〈 신청기관명 〉

❍ 개요

- 검증 신청 대상 식별 정보

  제품명, 버전, 신청기관, 배포예상 앱스토어 등 사항을 기입한다.

  (작성 예1. 식별정보)

서비스명	*모바일 테스트 앱 V1.X (하이브리드)*
신청 기관	*신청기관명*
서비스 구분	*대민서비스*
보안공통기반 사용	*미사용*
운영 환경 (프레임워크 등)	*구글 안드로이드 11(운영환경),* *jQuery Mobile, Sencha Touch 등(프레임워크)*
배포 예정일	*2021.XX.XX*
배포 앱스토어	*(구글) Play스토어, (애플) 앱스토어, (기타) 기타 민간스토어*

- 서비스 소개

  서비스 대상, 주요 제공 서비스 설명 등 기입

  (작성 예2. 서비스 소개)

구분	내용
서비스 대상	*지방세 검색 희망 사용자(대국민)*
주요 서비스 설명	*최근 3년간 지방세 납부 및 고지서 검색 등의 서비스 제공*

- 주요 라이브러리 사용 현황

  기타 추가적으로 포함되어야 할 사항(공개용·상용 라이브러리 사용 현황 등)

  (작성 예3. 라이브러리 사용 현황)

라이브러리	내용
open.lib	*- (출처) 오픈그래프 그룹* ** (URL) http://www.openlibrary_example.org* *- (기능) 그래프 작성 및 뷰어 기능* ** (위치) /lib/open.lib* ** 필요시, 컴파일시 주의사항 기술* *- (사용버전 / 배포일) / (최신 배포버전) 1.0.1(21.01.01.) / 1.0.2*
…	…

❶ 보안속성

- 일반적으로 다음의 사항을 포함한다.
  - 앱 기능 동작으로 처리되는 중요정보
  - 앱 처리정보 보호에 사용되는 암호화 알고리즘
  - 모바일 플랫폼에서 제공하는 보안메커니즘 사용 내역
  - 그 외 추가적으로 포함되어야 할 사항

(작성 예시)

<table>
<tr><th colspan="2">보안속성</th><th>내용</th></tr>
<tr><td rowspan="2">중요
정보</td><td>개인
정보</td><td>
<table>
<tr><th>구분</th><th>개인정보</th><th>보안조치</th><th>저장/전송 경로</th></tr>
<tr><td>수집</td><td>고유식별정보</td><td>정보주체 동의</td><td>/crm/sms/file1.java</td></tr>
<tr><td>저장</td><td>인증정보</td><td>해쉬값(SHA-256) 저장</td><td>/crm/sms/file2.java</td></tr>
<tr><td>전송</td><td>인증정보, 고유식별정보</td><td>암호화(AES) 전송</td><td>/crm/sms/file2.java</td></tr>
</table>
※ 수집, 저장, 전송되는 모든 개인정보(인증정보, 고유식별정보 등)를 기입하며, 해당사항이 없을 시에는 “해당사항 없음”이라고 명기
</td></tr>
<tr><td>위치
정보</td><td>
<table>
<tr><th>구분</th><th>개인정보</th><th>보안조치</th><th>저장/전송 경로</th></tr>
<tr><td>수집</td><td>개인위치정보(GPS)</td><td>위치정보주체 동의</td><td>/crm/sms/file1.java</td></tr>
<tr><td>저장</td><td>개인위치정보(GPS)</td><td>해쉬값(SHA-256) 저장</td><td>/crm/sms/file2.java</td></tr>
<tr><td>전송</td><td>개인위치정보(GPS)</td><td>암호화(AES) 전송</td><td>/crm/sms/file2.java</td></tr>
</table>
</td></tr>
<tr><td colspan="2">소스코드 난독화</td><td>☑ 적용 (상용 난독화 솔루션)　☐ 적용 안함
(예 : Proguard(무료), 상용 난독화 솔루션 등 적용 방식 기입)</td></tr>
<tr><td colspan="2">앱 위·변조</td><td>☑ 적용 (상용 위·변조 솔루션)　☐ 적용 안함
(예 : APK파일 해시값 검증, 상용 위·변조 솔루션 등 적용 방식 기입)</td></tr>
<tr><td colspan="2">보안메커니즘</td><td>• (iOS의 경우) 암호키 저장시 키체인 사용
• (공통기반 사용시) 전송데이터 암호화시, 공통기반 VPN 사용</td></tr>
<tr><td colspan="2">…</td><td>• 기타 참고사항 작성</td></tr>
</table>

❍ 구현기능

- 일반적으로 다음의 사항을 포함한다.
  - 구현된 기능동작 설명 및 기능에 사용되는 URL(사용 목적 포함) 기입
  - UI에서 식별되지 않는 기능(예, 서비스 등) 설명
  - Android 앱의 경우 해당 기능의 Activity명, 사용되는 intent-filter 기입
  - 소스코드 제공이 어려운 상용 또는 공개모듈 사용 시, 사용목적 및 기능 설명
  - 그 외 추가적으로 검증 시 고려되어야 할 사항

(작성 예시)

주요기능	기능 설명	비고
로그인	• *테스트 정보 입력 및 검색을 위한 적절한 사용자 여부 확인* *※ 필요시, 해당 메뉴 캡처 가능*	*(Activity) MainLogin* *(intent-filter) -*
…		

붙임 제3호 서식 접수증

모바일 전자정부서비스 앱 소스코드 검증 신청 접수증			
접 수 번 호			
접수담당자			
검증 신청인	기관명		
	성 명		
	연락처		
서 비 스 명			
위와 같이 접수하였음을 확인합니다. 년 월 일 한국인터넷진흥원		접수인	

※ 접수된 제출물은 내부 제출물 관리 절차에 의해 안전하게 관리됩니다.

붙임 제4호 서식 보완요청서

〈접수번호〉

모바일 전자정부서비스 앱 소스코드 검증 보완요청서

〈 검증대상 제품명 〉

년 월 일

KISA 한국인터넷진흥원

1. 개요

- 일반적으로 다음의 사항을 포함한다.
  - 검증신청 개요 : 접수번호, 검증대상 제품명, 신청기관명 등
  - 보완요청서 개요 : 보완요청서 식별정보, 보완요청 목록 등

2. 보완요청

- 보완요청 항목에는 일반적으로 다음의 사항을 포함한다.
  - 검증기준항목, 보완요청 내용 중 보안위협이 될 수 있는 사항
  - 기타 추가적으로 포함되어야 할 사항

(작성 예)

검증기준 항목	보완요청 내용	비고
FV-4. 중요정보 관리	• 비밀번호를 평문으로 전송함	결과 캡쳐 이미지
…		

붙임 제5호 서식 보완조치내역서

〈접수번호〉

모바일 전자정부서비스 앱 소스코드 검증 보완조치내역서

〈 검증대상 제품명 〉

년 월 일

〈 신청기관명 〉

1. 개요

- 일반적으로 다음의 사항을 포함한다.
  - 보완조치 대상 제품명, 신청기관명 등
  - 보완요청일, 보완조치기간 등

(작성 예)

서비스명	모바일 테스트 앱
신청기관	신청기관명
검증 신청/접수일	202x.xx.xx / 202x.xx.xx
보완요청 접수/제출일	202x.xx.xx / 202x.xx.xx
보완조치기간	202x.xx.xx ~ 202x.xx.xx

2. 보완조치

- 보완조치 항목에는 일반적으로 다음의 사항을 포함한다.
  - 보완요청 항목, 보완요청 내용에 대한 조치내역, 조치사항에 대한 자체 확인결과 등
  - 기타 추가적으로 포함되어야 할 사항

(작성 예)

보완요청 항목	보완요청 내용	조치사항
FV-4. 중요정보 관리	• 비밀번호 평문 전송	• 보안서버(SSL 서버) 구축을 통해 비밀번호 암호화 전송 * 관련 수정 소스코드 - src/ssl.java
…		

붙임 제6호 서식 결과보고서

〈접수번호〉

모바일 전자정부서비스 앱 소스코드 검증 결과보고서

〈 검증대상 제품명 〉

년 월 일

KISA 한국인터넷진흥원

제1장 개요

- 일반적으로 다음의 사항을 포함한다.
  - 앱 소스코드 보안약점·기능 보안취약점 검증 관련 규정
  - 검증대상 식별정보
  - 신청기관명, 검증기관명
  - 기타 추가적으로 포함되어야 할 사항

제2장 검증대상 제품 구조

- 일반적으로 다음의 사항을 포함한다.
  - 제품 구성 및 주요 기능 설명

제3장 검증결과

- 일반적으로 다음의 사항을 포함한다.
  - 검증대상의 소스코드 보안약점·기능 보안취약점 검증결과를 요약하여 기술
  - 특이사항 등
  - 기타 추가적으로 포함되어야 할 사항

[부록] 보완내역

- 일반적으로 다음의 사항을 포함한다.
  - 보완요청 목록(보완요청 항목, 처리상태 등) 등
  - 기타 추가적으로 포함되어야 할 사항

모바일 전자정부 앱 검증 신청기관을 위한

모바일 전자정부서비스
앱 소스코드 검증 가이드라인

인 쇄 2021년 10월
발 행 2021년 10월

발행처 행정안전부
세종특별자치시 한누리대로 411(어진동)
Tel : 02-2100-3399

한국인터넷진흥원
전라남도 나주시 진흥길 9
Tel : 061-820-2748

디자인/인쇄_예원디자인 www.yewondnp.com

비 매 품

모바일 전자정부 앱 검증 신청기관을 위한

모바일 전자정부서비스 앱 소스코드 검증 가이드라인

행정안전부

KISA 한국인터넷진흥원