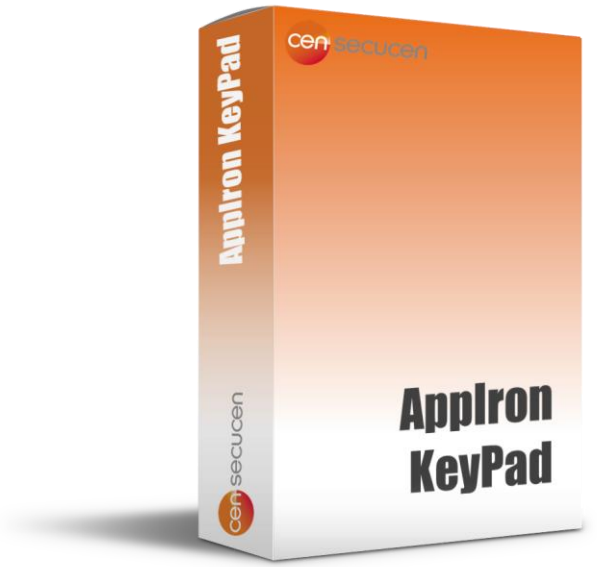
Creative | Energy | National Service

# AppIron KeyPad 표준 제안서

## 모바일 가상 키패드




Copyright © 2020 SECUCEN Co., Ltd. All rights Reserved | Confidential

(주)시큐센

# Contents

# 1. 제안 배경

## 모바일 가상 키패드의 필요성

### 키보드 입력값 탈취

- 금융서비스의 경우 계좌 비밀번호 등 사용자가 입력하는 정보의 민감도가 매우 높아 입력값이 탈취될 경우 큰 문제가 될 수 있음.
- 모바일 기기에서는 물리적인 키보드 입력값이 아닌 가상 키보드를 이용한 모바일 기기에서는 물리적인 키보드 입력이 아닌 가상키보드를 이용한 터치 이벤트를 통해 입력을 받기 때문에 사용자가 터치한 좌표 값으로 키 정보를 획득하거나, 스크린 캡처 등을 통해 사용자가 입력한 비밀번호가 유출될 수 있음.

### 보안 키보드

- 인증을 위한 중요정보(공인인증서 비밀번호, 계좌 비밀번호, 로그인 비밀번호 등) 입력시 키보드 후킹이나 좌표값 추출과 같은 입력값 탈취 공격으로부터 방어하기 위해 운영체제에서 제공하는 키보드가 아닌 앱 자체에서 보안 기능을 제공하는 키보드
- 화면에 표시되는 키보드 버튼의 배열을 다르게 표시, 고정 좌표값을 탈취하여 입력값을 유추하는 것을 막음.
- 현재는 입력값을 암호화하여 메모리 해킹을 이용한 비밀번호 평문을 탈취하지 못하도록 하거나, 보안 키보드가 동작하는 동안 화면을 캡쳐하지 못하도록 하는 등 방어 기능도 적용.

✓ 비밀번호는 노출되지 않도록 보호하는 것이 매우 중요
✓ 이를 위해 OS에 내장된 키보드가 아닌 가상 키패드와 같은 보안키패드를 적용하거나 키 로깅이 어렵도록 키보드 보안 모듈 적용 필요함.

# 1. 제안 배경

## 관련 법규에서 요구하는 가상키패드 보안

금융감독원의 『전자금융감독규정』, 『금융회사 정보기술(IT)부문 보호업무 모범규준』, 『스마트폰 전자금융서비스 주요 안전대책』 및 행정자치부의 『모바일 전자정부서비스 구축지침 및 가이드라인』에 의거하여 중요 입력 정보를 보호해야 합니다.

### 전자금융감독규정

- 제 34조 (전자금융거래 시 준수사항)
  ② 금융기관 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.
  3. 해킹 등 침해행위로부터 전자금융거래를 보호하기 위해 이용자의 전자적 장치에 보안 프로그램 설치 등 보안 대책을 적용할 것 (다만, 고객의 책임으로 본인이 동의하는 경우에는 보안 프로그램을 해제할 수 있다.)

  • 전자금융감독규정 해설서(개정판_2009.12)
  □ 전자금융 이용자가 전자적 장치(PC, 노트북)를 이용하여 금융기관 또는 전자금융업자의 전자금융 서비스에 접속하는 경우 우선적으로 이용자의 전자적 장치에 키보드 해킹방지 등의 보안 프로그램 또는 전자적 장치의 취약성을 보완할 수 있는 기타 보안기능을 제공

### 금융회사 정보기술(IT)부문 보호업무 모범규준

- Ⅲ. 정보기술부문 11. 해킹 등 침해행위 방지 대책
  ⑥ (이용자의전자적장치보호) 금융회사 등은 해킹 등 침해행위로부터 전자금융거래 및 관련 이용자 정보를 보호하기 위해 개인용컴퓨터(PC) 등 이용자의 전자적 장치에 보안프로그램 설치 등 보안대책을 적용하여야 한다.
  → 본인이 동의하는 경우에는 고객의 책임하에 보안프로그램 해제 가능

### 스마트폰 전자금융서비스 주요 안전 대책

- 2. 안전대책 나.기술적 침해대응 부분
  1) 비밀번호 등 중요입력정보가 유출되거나, 변조되지 않도록 입력정보 보호대책 적용

### 모바일 전자정부서비스 구축지침 및 가이드라인

7. 모바일 전자정부 서비스 보안 가이드라인
– 모바일 서비스 보안 위협 별 대책

| | 네트워크 |
|---|---|
| 위협 요소 | 접속의 불법적인 스니핑 |
| | MITM 공격 |
| 보안 대책 | 가상키보드 설치 (단말, 서버) |
| | E2E 암호화 솔루션 적용 |

행정안전부

## AppIron KeyPad 개요

AppIron KeyPad는 스마트폰을 위한 가상 키보드 보안 솔루션으로 전자금융거래 및 개인정보 보호와 동시에 사용자 편의성을 위한 인터페이스를 제공합니다.

| 구분 | 내용 |
|---|---|
| 제품명 | AppIron KeyPad |
| 제조사 | ㈜시큐센 |
| 제품 개요 | • 가상 키 패드를 이용한 중요정보 암호화<br>• 중요정보 유출 및 변조 방지 |

| OS | 최소사양 |
|---|---|
| Android | Android 4.0 이상 |
| iOS | iOS 6.0 이상 |

| 지원 알고리즘 | 내용 |
|---|---|
| 키생성 알고리즘 | DSA-SHA1-PRNG(FIPS-186-2 Appendix 3.1 , 3.3) |
| 대칭키 알고리즘 | AES 128bit |
| 비대칭키 알고리즘 | RSA 2048bit |
| 해쉬/위변조 방지 알고리즘 | HMAC(SHA1) |

| 주요기능 | 세 부 내 용 |
|---|---|
| 입력 값 보호 | • 모든 입력 정보는 좌표만으로 구성.<br>• 입력된 좌표는 암호화 되어 서버로 전달 됨.<br>• 암호화된 값은 세션키로 암호화 되어 서버에서 복호화 |
| 배열 랜덤화 | • Customize된 키 패드는 입력 요청시 마다 랜덤하게 생성 |
| 다양한 모드 지원 | • 문자 키 패드 모드, 숫자 키 패드 모드, 전체화면 모드, 팝업 모드 등 다양한 모드 지원 |
| 다양한 옵션 지원 | • 힌트 텍스트, 텍스트 색상, 배경 색상, 입력된 텍스트 색상, 화면 타이틀, 화면 설명 등 다양한 옵션 지원 |

# 2. AppIron KeyPad 소개

## 모바일 가상 키패드 솔루션 AppIron KeyPad

AppIron KeyPad는 스마트폰 모바일 앱을 위한 가상키패드 보안 솔루션으로 **중요 정보를 암호화**하여 **중요 정보가 유출되거나 변조되지 않도록 입력정보를 보호**함으로써 전자금융거래 및 개인정보 보호와 동시에 사용자 편의성을 위한 인터페이스를 제공합니다


+ 입력값의 위치값을 암호화 하여 전달합니다.
+ 모든 입력 정보는 좌표만으로 구성되어 있고, 이 또한 암호화 되어 있어 정보의 무결성을 보장합니다.

# 3. 주요 기능

## 동작 방식

AppIron KeyPad는 사용자마다 서로 다른 가상의 키패드를 생성해주는 **클라이언트**와 전달 받은 암호화 데이터를 복호화해주는 **라이브러리**로 구성되어 있습니다.


+ App에 입력요청이 들어오면 AppIron KeyPad Client는 랜덤 키패드를  생성합니다.
+ 키패드 입력이 끝이 나면 AppIron KeyPad Client는 암호화 된 값을 App에 전달합니다.
+ App은 전달받은 암호화 데이터를 KeyPad Server에 전달합니다.
+ 전달받은 암호화 데이터는 AppIron KeyPad Server에서 복호화 및 인증을 진행합니다

## 흐름도

AppIron KeyPad는 다음과 같은 흐름으로 구동됩니다.


+ App에서 가상키보드 호출 및 대칭키 생성을 SDK로 요청하게 되고, SDK는 사용자가 입력을 완료하면 암호화된 데이터를 반환합니다.
+ App은 반환받은 암호화 데이터 뿐만 아니라 전문을 App Server로 전달하게 됩니다.
+ App Server는 AppIron KeyPad Server를 통해 암호화 데이터를 복호화한 뒤, 사용자 입력값을 가지고 트랜잭션 처리를 합니다.
+ App Server에서 받은 결과에 따라 App은 다음 단계로 진행하게 됩니다.

# 4. 기대 효과

## AppIron KeyPad를 통한 기대 효과

### 보안적인 측면

#### 입력 값 보호

입력한 정보는 해당 정보의 좌표를 암호화하여 서버로 전달되므로 전송 중의 암호가 탈취되어도 정보가 유출되지 않으므로 무결성과 기밀성을 제공

#### 모바일 위협 대응

OS에 내장된 키보드가 아닌 보안 키패드를 적용함으로써 키 로깅, 스니핑 등에 대한 모바일 위협 대응이 용이

#### 배열의 랜덤화

Customize 된 키패드는 입력 요청시마다 매번 랜덤하게 키패드를 배열함으로써 더욱 안전하게 입력된 정보를 보호

**AppIron KeyPad를 통한 기대 효과**

### 편의적인 측면

#### 장애인 차별 금지법 대응

장애인을 정당한 이유 없이 배제 거부하거나 불리하게 대우하지 않음으로써 인간의 존엄과 가치를 구현

#### 다양한 모드 지원

문자 키 패드 모드, 숫자 키 패드 모드 등 다양한 모드를 지원

#### 다양한 옵션 지원

힌트 텍스트 제공 및 색상 변경 등 사용자마다 다양한 옵션을 지원함으로써 각기 다른 UI 적용 가능

# 5. ㈜시큐센 소개

## ㈜시큐센 개요

secu cen
(주)시큐센

### 주식회사 시큐센

대표자 박원규

- '12년 설립 후, 바이오 전자서명 사업을 전개해 온 "㈜시큐센"과, '11년 설립 후, 모바일 보안 솔루션/서비스 사업을 전개해 온 "바른소프트기술㈜"이, '15년 9월 통합 후, 아이티센의 보안부문 전문 계열사로 편입하여, 바이오 전자서명과 모바일 분야의 핀테크 보안 솔루션/서비스 전문기업으로 발전
- '18년 2월1일 아이티센의 금융권 모바일/창구 전자문서 구축분야 전문기업인 "㈜S&TC"를 흡수합병하여 "핀테크 보안기술 전문기업"으로 성장

**사업 분야 :** 보안솔루션(바이오전자서명, 인증, 모바일보안, 암호솔루션 외) 개발 및 공급, 금융디지털채널 구축 및 서비스, 보안 컨설팅

**자본금 :** 7억 1,562만원

**주소 :** 서울특별시 영등포구 가마산로 343 콤텍빌딩 3층

**전화번호 :** 02-3495-0700

**팩스 :** 02-521-6275

**회사설립일시 :** 2011년 12월 7일

**부문종사기간 :** 2011년 12월 ~ 2020년 4월 현재 ( 8년 4개월 )

### 주 요 연 혁

2011~2020

**2020**
- 현대카드 블록체인기반 DID APP 구현 사업 수주 및 진행

**2019**
- 금결원『바이오분산관리 전자서명 기술지원 및 이용기관 연계 협약』체결
- (주)알체라『바이오 전자서명·인증관련 인식기술 제휴계약』체결

**2018**
- 주식회사 에스엔티씨 합병
- 기술혁신형 중소기업(Inno-Biz)선정

**2017**
- 라이나 금융 방화벽정책관리 시스템 구축 사업 수주
- 나이스 학교생활기록부 ISP 사업 수주
- 하나금융티아이 '바이오 전자서명' 사업협약 체결

**2016**
- 국토교통부 '부동산안전거래 통합지원시스템' '바이오 전자서명' 수주
- 공정위 소비자피해구제 종합지원시스템 구축(정보보호시스템) 사업 수주
- 에듀파인시스템 응용SW 유지보수사업 수주(보안컨설팅)
- 기획재정부 국고보조금 통합관리시스템 구축사업 수주(정보보호분야)

**2015**
- 전북은행FDS(이상거래탐지시스템) 수주 및 구축완료
- LGU+Pay Now FDS 수주 및 구축완료

**2015**
- 전화번호 안심로그인 서비스 공동사업제휴/런칭('16.1)
- SK그룹사 APT대응솔루션 구축사업 수주
- 금융위원회, 제5차 핀테크 Demo-Day 선정 및 발표
- 아이티센 자회사로 편입

**2014**
- '바이오 전자서명' 공인인증기술 지정 위한 사전심사 진행
- 외환은행 FDS 프로젝트 수주 및 구축완료
- 롯데카드 안심쇼핑 세이프인증서 부가서비스 런칭

**2013**
- 안행부 모바일 공통기반 앱보안시스템 구축
- '바이오 전자서명' 특허 3건 등록 및 GS인증 획득
- 스마트폰 도용방지 서비스 출시
- 경남은행 차세대 인터넷 뱅킹 시스템 구축사업 참여

**2012**
- 외환은행 인터넷뱅킹 앱 위변조방지/난독화 수주/구축

**2011**
- 법인 설립

## ㈜시큐센 제품 및 서비스 로드맵(1/2)

시큐센은 다양한 모바일 핀테크 응용서비스 환경에서 사용자에게 보다 안전한 서비스를 제공하기 위한 핀테크 보안 솔루션, 인증, 전자서명 솔루션 및 서비스를 제공합니다.

### 바이오 전자서명 – DocuTrust

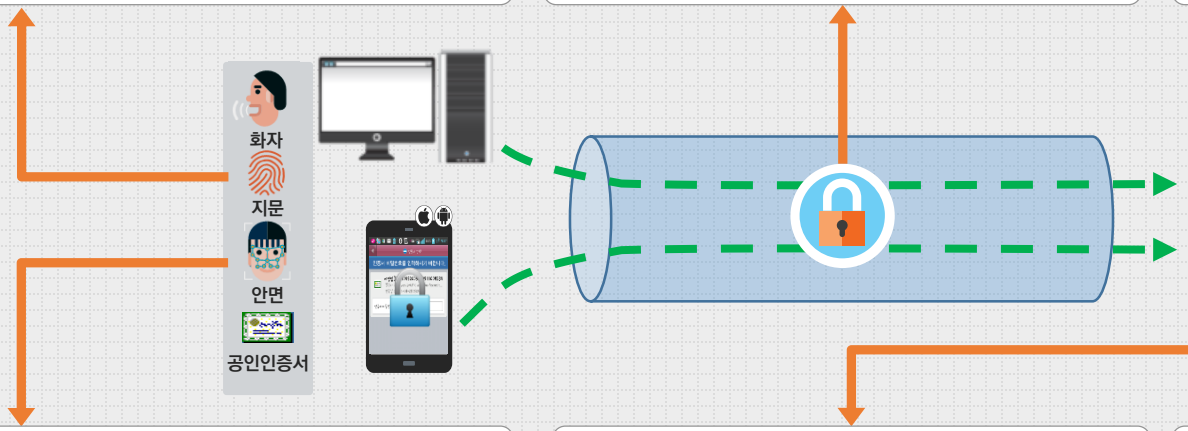

- **제조사 :** 시큐센(국산)
- **주요기능**
  바이오 전자서명 플랫폼으로 고객사가 원하는 바이오 정보를 사용하여 안전한 서명을 지원.

### 구간암호화 – EnXection


- **제조사 :** 시큐센(국산)
- **주요기능**
  Server-Server, Server-Client 환경에서의 구간암호화 지원 라이브러리 형태로 제공

### 모바일 앱위변조방지 – AppIron


- **제조사 :** 시큐센(국산)
- **주요기능**
  모바일 앱위변조 방지 솔루션 역공학, Debugging 방지 바이너리 난독화 제품 동시 보유




### 바이오 인증 플랫폼 – EdgeBio


- **제조사 :** 시큐센(국산)
- **주요기능**
  안면인증을 통한 인증/전자서명 구간암호화,데이터 분산저장 지원 인증매체와의 독립성을 보장

### 모바일 가상키패드 – AppIron KeyPad


- **제조사 :** 시큐센(국산)
- **주요기능**
  스마트폰을 위한 가상 키보드 보안 솔루션. 전자금융거래 및 개인정보 보호와 사용자에게 편리한 UI 제공.

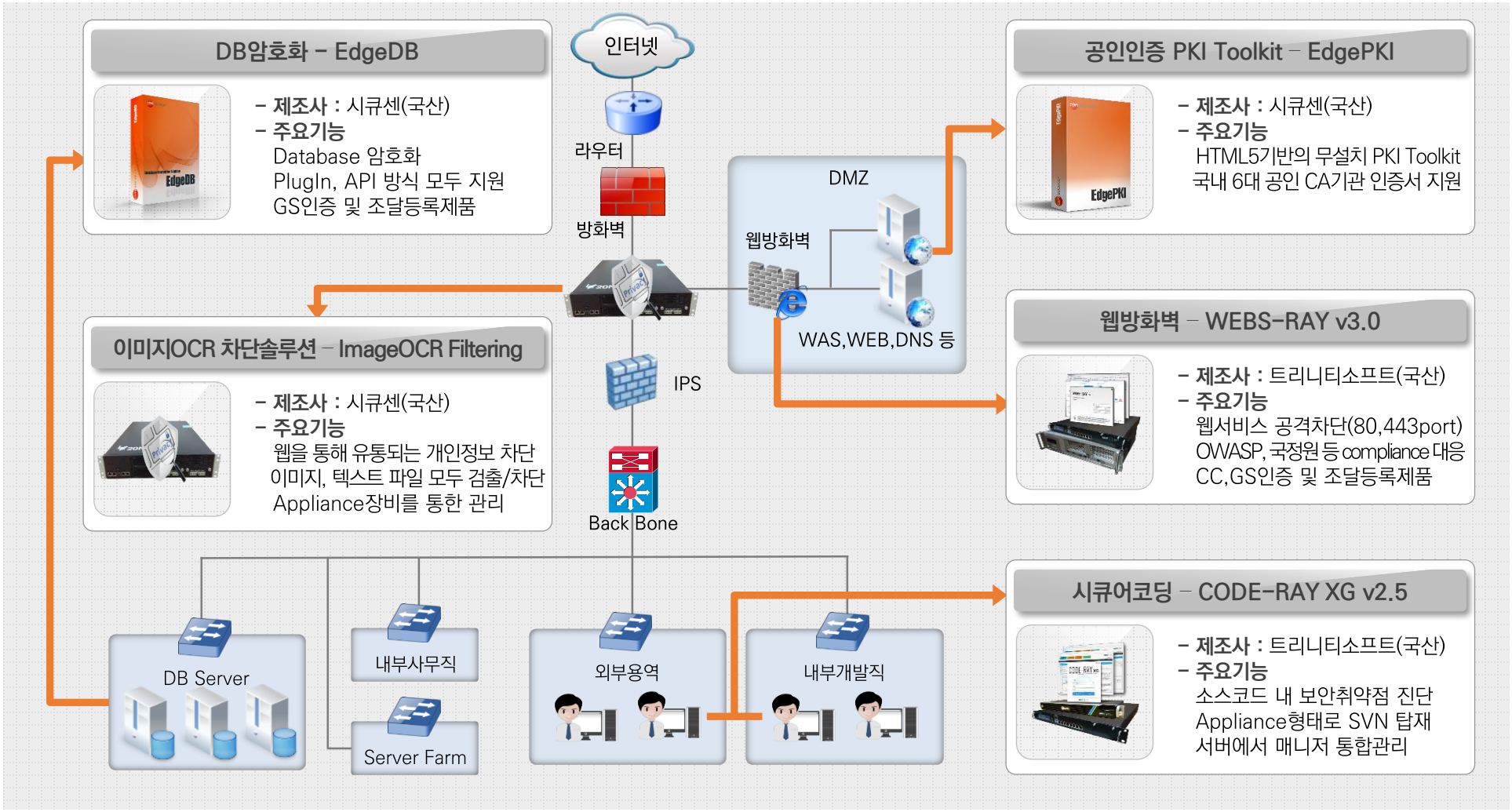
### 모바일 백신– AppIron Vaccine


- **제조사 :** 시큐센(국산)
- **주요 기능**
  모바일 백신 솔루션을 Embeded 형식으로 제공함으로써 사용자가 별도의 설치 없이 사용 가능

# 5. ㈜시큐센 소개

## ㈜시큐센 제품 및 서비스 로드맵(2/2)

시큐센은 개인정보보호를 위하여 컨설팅 서비스를 고객사에게 제공하고 있습니다. 이에 기술적인 보호를 위한 정보보호 제품을 구축, 지원하여 사업을 수행하고 있습니다.



서울특별시 영등포구 가마산로 343 콤텍빌딩
343, Gamasan-ro, Yeongdeungpo-gu, Seoul, Republic of Korea
TEL+82-2-3495-0700 FAX+82-2-521-6275

WWW.SECUCEN.COM

시큐센
secucen