신용카드 회원의 정보보호를 위한

단말기 시험 가이드

2018. 1. 25

여 신 금 융 협 회

단말기시험-가이드-001(00)-비접촉식 신용카드 단말기 시험요구사항

문서 식별	단말기시험-가이드-001(00)
문서 제목	비접촉식 신용카드 단말기 시험요구사항
개정 이력	00 (최초), 2018년 1월 25일
적용 일자	2018년 2월 1일
공개 범위	☑ 인증기관 ☑ 시험기관/시험업무 수탁기관 ☑ 신청기관

■ 문서개요

- **[발행목적]**
  - 다양한 형태의 비접촉식 신용카드 단말기 시험에 적용해야할 세부 요구사항을 제시함

- **[적용범위]**
  - Contactless EMV 거래를 수행하는 비접촉식 신용카드 단말기
  - Contactless EMV 거래를 수행하지 않는 비접촉식 신용카드 단말기
  - Contactless EMV 거래를 수행하지 않는 비접촉식 신용카드 전용 카드리더기

■ 세부가이드

신용카드 단말기 정보보호 기술기준을 원칙적으로 적용하되, 다음의 해당되는 경우에는 비접촉식 단말기 시험요구사항을 만족해야 한다.

- [비접촉식-01] 비접촉식 전용 카드리더기가 Contactless EMV 거래를 수행하는 경우, Contactless EMV 인증(Level1/브랜드별 Level2)을 받아야 함
- [비접촉식-02] Contactless EMV 거래를 하지 않는 비접촉식 거래만 지원하는 단말기는 EMV 인증에 준하는 방식으로 신용카드 거래의 안전성 및 호환성을 보장해야 함(예: T-money, JUSTOUCH 등, 인증기관과 사전에 협의된 방식 등)
- [비접촉식-03] 사용 시간과 사용 횟수에 제한이 있는 형태(예: 가상신용카드번호, 토큰, OTC 등)의 신용카드번호는 민감한 신용카드 정보로 분류되지 않으며, 앱카드에서 이러한 형태의 신용카드번호만 취급하는 경우(그 외 민감한 신용카드 정보를 사용하지 않는 경우)에는 신용카드 단말기 기술기준의 적용범위에서 제외

단말기시험-가이드-002(00)-POS 단말기 등록 범위 적용

문서 식별	단말기시험-가이드-002(00)
문서 제목	POS 단말기 유형에 따른 단말기 등록 범위 적용
개정 이력	00 (최초), 2018년 1월 25일
적용 일자	2018년 2월 1일
공개 범위	☑ 인증기관 ☑ 시험기관/시험업무 수탁기관 ☑ 신청기관

■ 문서개요

- **[발행목적]**
  - 다양한 POS 단말기 유형이 존재함에 따라 POS 단말기 등록 범위 적용에 일관성을 제고하기 위해 기준을 제시함

- **[적용범위]**
  - 특수한 형태의 POS 단말기(전기차, 주유소 등)를 제외한 모든 종류의 POS 단말기

- **[용어정의]**
  - "**POS 단말기 등록 범위**"는 POS 단말기의 형상을 유지·관리하기 위하여 시험결과보고서에 기재하는 POS 단말기의 물리적 범위를 의미한다.
  - **"일체형 POS 단말기"**는 POS 단말기 본체 내에 카드리더기가 내장된 형태의 단말기를 의미한다.
  - **"범용 OS"**는 최종 사용자가 별도로 구하여 설치할 수 있는 신뢰된 운영체제로 주기적 보안 패치가 이루어지는 운영체제를 의미한다.

    (예: MS Windows 7, MS Windows 8 등)
  - **"전용 OS"**는 개발사에서 만든 OS 또는 범용 OS를 기반으로 수정이 이루어진 운영체제를 의미한다.

    (예: RTOS, Linux 기반 자체OS 등)

■ 세부 가이드

POS 단말기의 유형에 따라 단말기 등록 범위를 적용하기 위해서 아래

와 같이 POS 단말기 유형을 분류함

1) POS 본체와 카드리더기가 물리적으로 분리된 경우

① POS 본체가 범용 OS를 사용하는 경우

② POS 본체가 전용 OS를 사용하는 경우

2) 카드리더기가 POS 본체에 포함된 경우

① POS 본체가 범용 OS를 사용하는 경우

② POS 본체가 전용 OS를 사용하는 경우

POS 단말기의 유형에 따라 등록 범위를 아래와 같이 적용

1) POS 본체와 카드리더기가 물리적으로 분리된 경우

구분	단말기 등록 범위			
	POS 본체 외관	POS 본체 HW	카드리더기 외관	카드리더기 HW
(POS 본체)범용 OS	비대상	비대상 (최소 사양 기술)	대상	대상
(POS 본체)전용 OS	대상	대상	대상	대상

※ 단, 운영환경 식별의 용도로 범용 OS인 경우, 시험기관은 POS 본체에 대한 정보를 보고서에 기재함

2) 카드리더기가 POS 본체에 포함된 경우

구분	단말기 등록 범위			
	POS 본체 외관	POS 본체 HW	카드리더기 외관	카드리더기 HW
(POS 본체)범용 OS	대상	대상	N/A	대상
(POS 본체)전용 OS	대상	대상	N/A	대상

※ 단, 범용 OS를 사용하는 POS 단말기에서 『내·외부를 구분할 수 있는 물리적 외관을 가진 카드리더기』가 POS 본체에 포함된 경우, 'POS 본체의 외관' 및 'POS 본체 HW'를 단말기 등록 대상범위에서 제외할 수 있다.

(HW 사양을 "~이상"으로 표기 가능)

일체형 POS 단말기 시험허용에 대한 적용기준

● 다음의 적용기준에 따라 일체형 POS 단말기에 대한 시험가능 여부를 판단함

적용	형태	비고
허용	o POS 소프트웨어와 카드리더기가 **물리적으로 분리된 별도의 PCB에 설치**되고, 각 PCB는 POS 소프트웨어 또는 카드리더기의 **독립적인 보안기능을 수행**하는 경우	※전원부 공유는 가능함 ※일체형 POS 단말기에서 POS 소프트웨어와 카드리더기간 통신은 일반적인 POS 소프트웨어와 카드리더기 간 통신규격 및 방법을 동일하게 이용하여야 함
불허	o POS 소프트웨어 및 카드리더기가 **독립적인 보안기능을 가지지 않는 PCB에 설치**되어 개발된 형태일 경우	※독립적인 보안기능을 가지지 않는 PCB란, 각 PCB에서 POS 소프트웨어 또는 카드리더기의 보안기능을 단독으로 수행하지 못하는 형태를 의미함
불허	o **POS 소프트웨어 및 카드리더기가 하나의 PCB에 설치**되어 개발된 형태일 경우	※독립적인 보안기능을 가지지 않는 PCB에 설치된 것으로 간주함

단말기시험-가이드-003(00)-모바일 단말기 시험요구사항

문서 식별	단말기시험-가이드-004(00)
문서 제목	모바일 단말기 시험요구사항
개정 이력	00 (최초), 2018년 1월 25일
적용 일자	2018년 2월 1일
공개 범위	☑ 인증기관 ☑ 시험기관/시험업무 수탁기관 ☑ 신청기관

■ 문서개요

- **[발행목적]**

  - 모바일 단말기(Android OS, Apple iOS에서 변경시험 기준을 포함하여 모바일用 단말기 시험요구사항을 제시함

- **[적용범위]**

  - 운영체제가 “Android OS” 및 “Apple iOS”인 단말기

- **[모바일 운영체제 구분 체계]**

  - **(안드로이드)** 커널 버전, API 레벨, OS 버전, 코드 네임 등으로 표기됨

구분	Code Name	커널 버전	OS 버전	API 레벨
1	Cupcake	2.6.27	1.5	3
2	Donut	2.6.29	1.6	4
3	Eclair	2.6.29	2.0 ~ 2.1	5 ~ 7
4	Froyo	2.6.32	2.2 ~ 2.2.2	8
5	Gingerbread	2.6.35	2.3 ~ 2.3.7	9 ~ 10
6	Honeycomb	2.6.36	3.0 ~ 3.2.6	11 ~ 13
7	IceCreamSandwich	3.0.1, 3.0.8	4.0 ~ 4.0.4	14 ~ 15
8	JellyBean	3.0.31, 3.0.53, 3.4	4.1 ~ 4.3.1	16 ~ 18
9	KitKat	3.4	4.4 ~ 4.4.4	19
10	Lollipop	3.4	5.0 ~ 5.1.1	21 ~ 22
11	Marshmallow	3.10.83	6.0, 6.0.1	23
12	Nougat		7.0~7.1.2	
13	Oreo		8.0~	

- (Apple iOS) iOS 이름, iOS 버전, 빌드 번호 등으로 표기됨

구분	OS 이름	OS 버전	빌드 번호
1	iPhone OS 1	1 ~ 1.1	1XXX
2	iPhone OS 2	2 ~ 2.2.1	5XXXX
3	iPhone OS 3	3 ~ 3.2.2	7XXXX
4	iOS 4	4 ~ 4.3.5	8XXXX
5	iOS 5	5 ~ 5.1.1	9XXXX
6	iOS 6	6 ~ 6.1.6	10XXXX
7	iOS 7	7 ~ 7.1.2	11XXXX
8	iOS 8	8 ~ 8.4.1	12XXXX
9	iOS 9	9 ~ 9.3.2	12XXXX
10	iOS 10		
11	iOS 11		

■ 세부 가이드

안드로이드 OS/애플 iOS 운영체제 기반 신용카드 단말기는 다음과 같은 시험요구사항을 만족해야 한다.

- [모바일-01] 운영체제에 대하여 안드로이드는 Code Name 기준(예: KitKat, Lollipop 등), Apple iOS는 OS 이름(예: iOS 9, iPhone OS 3 등) 기준으로 제출문서에 사양을 명시해야 함

※ 기인증된 POS 소프트웨어와 보안기능을 수행하는 소스코드가 동일한 경우에 한하여 변경시험 대상에서 제외함

- [모바일-02] (루팅 탐지) 운영체제의 변조(루팅, 탈옥 등)를 탐지 및 대응 기능을 제공해야 함
- [모바일-03] (자체보호) 보안기능 관련 저장데이터(보안기능 관련 프로그램 설정값 등) 변경 여부를 탐지하기 위해 앱에 대한 무결성 점검 기능을 제공해야 함

단말기시험-가이드-004(00)-키인거래 단말기 시험요구사항

문서 식별	단말기시험-가이드-005(00)
문서 제목	키인거래 단말기 시험요구사항
개정 이력	00 (최초), 2018년 1월 25일
적용 일자	2018년 2월 1일
공개 범위	☑ 인증기관 ☑ 시험기관/시험업무 수탁기관 ☑ 신청기관

■ 문서개요

- **[발행목적]**

- Key-In거래(이하 '키인거래') 방식을 지원하는 신용카드 단말기 시험에 적용해야할 세부 요구사항을 제시함

- **[적용범위]**

- 수기입력 방식의 키인거래를 지원하는 신용카드 단말기

- **[용어정의]**

- **"KeyIn거래(키인거래)"**란 신용카드사와 가맹점간 수기특약 등에 의해 단말기 화면에서 수기입력된 일부 민감한 신용카드 정보(신용카드번호, 유효기한)를 이용하여 신용거래를 수행하는 형태를 의미한다.

- **"수기특약"**이란 가맹점 업종 특성(예약, 통신판매 등)에 의해 카드 실물의 압인 또는 접촉 없이 신용카드번호 및 유효기한을 수기로 작성하고 회원의 서명이 생략된 형태로 승인을 받은 후 신용카드 매출전표를 정상적인 매출전표로 인정하여 처리하도록 신용카드사와 가맹점간 체결된 계약을 의미한다.

- 세부가이드 "**적용방법**"에 명시된 기호(○, △) 의미는 다음과 같다.

  · ○ 키인거래 방식을 지원하는 단말기 시험에 해당 요구사항을 모두 적용

  · △ 키인거래 방식을 지원하는 단말기 특성을 고려하여 해당 요구사항을 적용(비고 참조)

■ 세부 가이드

키인거래 방식을 지원하는 신용카드 단말기는 다음과 같이 구분한다.

대면거래 여부	민감한 신용카드 정보 보호 수행 여부	인증등록 여부
대면거래	카드리더기 및 CAT 단말기를 통한 보호 수행	인증등록 대상
비 대면거래	카드리더기 및 CAT 단말기를 통한 보호 수행	인증등록 대상
비 대면거래	카드리더기 및 CAT 단말기를 통한 보호 수행하지 않음	인증등록 대상 제외 (예시 : 인터넷 상거래, 홈쇼핑 등)

키인거래 방식을 지원하는 신용카드 단말기는 정보보호 기술기준을 원칙적으로 적용하되, 다음과 같은 시험요구사항을 만족해야 한다.

CAT/POS 단말기 보안기능 및 시험요구사항		적용 방법	비고
5.1 민감한 신용카드 정보 보호	5.1.1	△	(다음의 요구사항 적용) (1)CAT/POS 단말기 화면에서 수기입력된 일부 민감한 신용카드 정보는 112비트 이상의 보안강도 암호알고리즘을 이용하여 CAT 단말기 내부 또는 카드리더기 내부에서 암호화 하여야 한다. (2)112비트 이상의 보안강도로 암호화된 민감한 신용카드 정보는 CAT/POS 단말기와 통신하는 VAN사 서버에서만 신용카드 거래 요청의 목적으로 복호화 될 수 있다. (3)통신 중계 등을 목적으로 CAT/POS 단말기 본체로부터 VAN사 서버까지의 일부 민감한 신용카드 정보 전송구간 상에 존재하는 어떠한 서버(예-EDI 가맹점 중계서버)도 암호화된 일부 민감한 신용카드 정보를 복호화 할 수 없다.
	5.1.2	O	(모든 요구사항 적용)
5.2 암호 연산 및 암호키 생성/분배	5.2.1, 5.2.2	O	(모든 요구사항 적용)
5.3 암호키 접근 통제 및 파기	5.3.1, 5.3.2	O	(모든 요구사항 적용)
5.4 신용카드 번호 보호	5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.4.5	O	(모든 요구사항 적용)
5.5 자체보호	5.5.1, 5.5.2	O	(모든 요구사항 적용)