
신용카드 회원의 정보보호를 위한

단말기 시험 가이드

2023. 8. 1

여 신 금 용 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	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 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	<ul style="list-style-type: none"> ○ POS 소프트웨어와 카드리더기가 물리적으로 분리된 별도의 PCB에 설치되고, 각 PCB는 POS 소프트웨어 또는 카드리더기의 독립적인 보안기능을 수행하는 경우 	<ul style="list-style-type: none"> ※전원부 공유는 가능함 ※일체형 POS 단말기에서 POS 소프트웨어와 카드리더기 간 통신은 일반적인 POS 소프트웨어와 카드리더기 간 통신규격 및 방법을 동일하게 이용하여야 함
불허	<ul style="list-style-type: none"> ○ POS 소프트웨어 및 카드리더기가 독립적인 보안기능을 가지지 않는 PCB에 설치되어 개발된 형태일 경우 	<ul style="list-style-type: none"> ※독립적인 보안기능을 가지지 않는 PCB란, 각 PCB에서 POS 소프트웨어 또는 카드리더기의 보안기능을 단독으로 수행하지 못하는 형태를 의미함
불허	<ul style="list-style-type: none"> ○ POS 소프트웨어 및 카드리더기가 하나의 PCB에 설치되어 개발된 형태일 경우 	<ul style="list-style-type: none"> ※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	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

- [발행목적]

- 모바일 단말기(Android OS, Apple iOS에서 변경시험 기준을 포함하여 모바일용 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	4.4.1	7.0~7.1.2	24 ~ 25
13	Oreo	4.10	8.0, 8.1~	26

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

구분	OS 이름	OS 버전	빌드 번호
1	iPhone OS 1	1 ~ 1.1	1A543a ~ 1C28 3A100a ~ 4B1
2	iPhone OS 2	2 ~ 2.2.1	5A347 ~ 5H11a
3	iPhone OS 3	3 ~ 3.2.2	7A341 ~ 7B500
4	iOS 4	4 ~ 4.3.5	8A293 ~ 8L1
5	iOS 5	5 ~ 5.1.1	9A334 ~ 9B208
6	iOS 6	6 ~ 6.1.6	10A403 ~ 10B500
7	iOS 7	7 ~ 7.1.2	11A465 ~ 11D257
8	iOS 8	8 ~ 8.4.1	12A365 ~ 12H321
9	iOS 9	9 ~ 9.3.5	13A340 ~ 13G36
10	iOS 10	10 ~ 10.3.3	14A403 ~ 14G60
11	iOS 11	11 ~	15A372 ~

■ 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	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 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 파괴	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)

단말기시험-가이드-005(00)-타 법령상 보안 기준 적용 장치

문서 식별	단말기시험-가이드-005(00)
문서 제목	타 법령상 보안 기준 적용 장치 간이 등록 절차 안내
개정 이력	00 (최초), 2018년 4월 30일
적용 일자	2018년 5월 8일 ~ 2020년 7월 20일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

● [발행목적]

- 「여신전문금융업법」에서 다루는 신용카드 단말기 임에도 불구하고, 타 법령상의 장치로서 보안 등 안전성 기준이 적용된 장치에 대한 간이등록 절차 안내

● [적용범위]

- 「계량에 관한 법률」의 규제를 받는 셀프주유기 및 가스 충전기
- 「전기용품 및 생활용품 안전관리법」 및 「전파법」에 따른 KC인증과 전자파인증 대상인 키오스크
- 「전자금융거래법」의 규제를 받는 자동화기기(CD/ATM) 중 신용카드를 통한 국세·지방세 납부 지원 장치

■ 세부가이드

여신전문금융업법 이외 타 법령상의 의무를 준수해야 하는 신용카드 단말기는 다음 기준을 따라야 한다.

- [셀프주유기 및 가스충전기] 계량기로서 「계량에 관한 법률」에 의한 검정기관의 봉인을 받아 물리적으로 관리되고 있는 점을 감안하여, 주유기 등과 연동된 POS S/W에 카드거래 정보 저장되지 않도록 추가 조치 등을 한 후 간이식별번호(유효기간 2년)를 부여받아 등록
 - 단, 해당 제품을 사용하는 가맹점주는 「신용카드 단말기 시험·인증 및 등록관리 규정」 별지 제19호 서식에 따른 ‘가맹점주 자체점검 표시양식’을 카드리더기 주변에 부착후 매월 정기점검 하여야 한다.
- [카드단말기(리더기)·분체 분리가능형 키오스크] 카드단말기(리더기)는 반드시 등록된 제품을 사용하되, POS S/W는 카드거래 정보 저장 안되도록 추가 조치 등을 한 후 간이식별번호(유효기간 6개월)를 부여받아 등록
- [자동화기기(CD/ATM)] MS전용 카드 거래가 전면 금지된 점을 감안하여, 인증기관 등에 국세·지방세 신용카드 납부 자동화기기 등록 신청서 제출하여 등록

단말기시험-가이드-006(00)-고정형 토큰 사용 비접촉식 단말기

문서 식별	단말기시험-가이드-006(00)
문서 제목	고정형 토큰 사용 비접촉식 단말기
개정 이력	00 (최초), 2018년 4월 30일
적용 일자	2018년 5월 8일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

- [발행목적]
 - 사용시간과 횟수에 제한이 없는 형태의 신용카드 번호를 사용하는 장치에 대한 기준 안내
- [적용범위]
 - 고정형 토큰(가상 신용카드 번호)을 사용하는 비접촉식 전용 단말기 (예 : 바코드/QR코드 전용리더기, 삼성페이 전용 사인패드 등)

■ 세부가이드

사용 시간과 사용 횟수에 제한이 없는 고정형 토큰*을 사용 하더라도, 비접촉식 전용 장치에 한하여 실제 카드정보가 아닌 점을 감안하여 민감한 신용카드 정보를 사용하지 않는 장치로 분류한다.

* 단, 가상 카드번호를 사용해야 함

구분	단말기 등록	비고
접촉식 기능 지원	대상	
비접촉식 전용	비대상	단, 실제 카드정보 처리 불가

※ 고정형 토큰에 사용된 가상 카드번호와 유효기간으로 Key-in 승인은 허용되지 않음

단말기시험-가이드-007(00)-특수유형 셀프주유기 및 가스충전기

문서 식별	단말기시험-가이드-007(00)
문서 제목	특수유형 셀프주유기 및 가스충전기
개정 이력	00 (최초), 2018년 7월 5일
적용 일자	2018년 7월 5일 ~ 2020년 7월 20일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

• [발행목적]

- 타법령상 보안 기준 적용 장치로서 간이 등록 대상인 셀프주유기 및 가스충전기와 관련하여 특수형태로 구성된 POS에 대한 추가 조치 필요사항을 제시

• [적용범위]

- 셀프주유소/가스충전소에 설치된 간이등록 대상 POS S/W가 CAT 단말기 및 SC장치(Site Controller) 등을 통해 부가통신업자(이하 'VAN사')와 통신하는 경우

■ 세부가이드

셀프주유소/가스충전소에서 VAN사간 통신을 POS에 연결된 CAT단말기 및 SC장치* 등으로 하는 경우에 한하여, ODT**와 POS S/W에 부여할 간이 등록 식별번호를 VAN사 서버에서 생성하여 승인 요청전문에 반영하는 것을 허용

* 주유기/충전기/ODT 등과 POS사이에 설치되어 통신을 중계하는 장치

** Out Door Terminal : 주유기에서 신용카드 리딩을 수행하는 장치

o 단, 본 조치는 위와 같은 구성으로 카드결제가 이뤄지는 일부 POS제조사*의 제품을 사용하는 셀프주유소와 가스충전소만 적용 대상임

* 동화프라임, 미래전자 및 장위데이터 등 (가나다 순)

※ 각 VAN사는 POS와 연결된 CAT단말기가 셀프주유소/가스충전소 이외의 타 사업장에서 사용되지 않도록 유의

단말기시험-가이드-008(01)-블루투스 단말기 시험요구사항

문서 식별	단말기시험-가이드-008(01)
문서 제목	블루투스 지원 단말기 시험요구사항
개정 이력	01 (개정), 2019년 10월 31일
적용 일자	2019년 11월 11일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

• [발행목적]

- 블루투스(Bluetooth) 통신을 지원하는 신용카드 단말기에 대한 보안 요구사항을 제시함

• [적용범위]

- 신용카드 거래를 위해 카드리더기와 POS S/W 연결 구간을 블루투스 통신으로 지원하는 신용카드 단말기(이하, 블루투스 단말기)

■ 세부가이드

• [블루투스 단말기 요구사항 및 제약사항(1)]

- 블루투스 단말기를 통하여 평문의 신용카드 번호를 전송하는 경우 블루투스 SIG* 인증을 득해야 함

* Bluetooth Special Interest Group

※ 암호화 또는 마스킹된 신용카드 번호를 전송하는 경우 해당사항 없음

• [블루투스 단말기 요구사항 및 제약사항(2)]

블루투스 단말기는 사용자가 사용하고자 하는 단말기임을 식별하기 위해 블루투스 최초 연결시 다음과 같은 사항을 만족해야 한다.

형태	보안 요구사항
LCD가 있는 카드리더기	<p>※POS 단말기 본체와 연동 시 LCD를 통하여 랜덤번호를 표시하고 POS 단말기 본체에서 랜덤번호를 입력하는 기능 탑재</p> <p>※또는 카드리더기 개체별 식별이 가능한 고유값을 표시하고, POS 단말기 본체에서 해당 값을 입력할 수 있는 기능 탑재</p>

LCD가 없는 카드리더기	프린터 존재함	※프린터 출력기능을 통하여 랜덤번호를 출력하고 POS 단말기 본체에서 랜덤번호를 입력하는 기능 탑재 ※또는 카드리더기 개체별 식별이 가능한 고유값을 출력하고, POS 단말기 본체에서 해당 값을 입력할 수 있는 기능 탑재
	프린터 존재하지 않음	※카드리더기 개체별 식별이 가능한 고유값을 POS 단말기 본체에서 입력할 수 있는 기능을 탑재

※ 단, 블루투스 단말기 기능 및 운영 환경상 상기 요구사항을 만족하지 못하는 경우 신청기관 등은 해당 단말기에서 블루투스 연결이 잘못되어 결제 사고가 발생하지 않도록 다음과 같은 보호방안을 마련해야 한다.

- 사용자가 사용하고자 하는 신용카드 단말기를 식별하고 입력할 수 있는 기능 구현

단말기시험-가이드-009(03)-스마트폰 단독 단말기 시험요구사항

문서 식별	단말기시험-가이드-009(03)
문서 제목	스마트폰 단독 단말기 시험 요구사항
개정 이력	03 (개정), 2023년 6월 15일
적용 일자	2023년 6월 19일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

• [발행목적]

- 스마트폰 단독 신용카드 단말기의 민감한 신용카드 정보 및 신용카드 번호 암호화를 위한 암호화 연산 및 암호키 요구사항을 제시

• [적용범위]

- 스마트폰에 POS S/W에 해당하는 앱(App.)만 설치하고, 카드리더기는 별도로 부착하거나 연동하지 않고 스마트폰에 내재된 카메라나 NFC 기능을 사용하는 스마트폰 단독 단말기*

* 신용카드 단말기 정보보호 기술기준의 CAT단말기 또는 카드리더기로 간주

• [단말기시험-가이드-010과의 관계]

- 스마트폰 단독 단말기 인증을 위해서는 단말기시험-가이드-009 및 단말기시험-가이드-010을 모두 충족하여야 함

■ 세부가이드

스마트폰 단독 단말기가 「신용카드 단말기 정보보호 기술기준」 제3장 제4절의 ‘2. 초기 암호키 주입에 대한 요구사항’ 및 제3장 제3절의 ‘3. 암호화에 대한 보안요구사항’ 을 준수하기 위해 아래 조건을 모두 만족해야 함

- o 민감한 신용카드 정보 및 신용카드 번호 암호화를 위해 사용되는 암호키를 생성·유도하기 위한 초기키는 안전한 방법으로 주입되어야 하며, 스마트폰

운영 환경에 노출되지 않아야 함

- 민감한 신용카드 정보 및 신용카드 번호 암호화를 위해 사용되는 암호키는 국내외 전문기관에서 안전성을 검증 받은 스마트폰의 보안시스템*의 보안 메커니즘에 의해 접근통제 되어야 하며, 암호키가 사용되고 저장되는 전체 과정에서 기밀성과 무결성을 확보해야 함

* 신뢰할 수 있는 실행환경(TEE), 보안요소(SE/eSE) 등

- 앱(App.)이 실행되는 REE와 보안시스템 사이의 통신은 안전한 채널을 생성하여 수행되어야 함
- 앱(App.)과 스마트폰 보안시스템은 증명(Attestation)을 수행해야하며, 증명 오류가 발생하는 경우 신용카드 결제기능 동작을 중지해야 함

단말기시험-가이드-010(03)-스마트폰 단독 단말기 시험요구사항(2)

문서 식별	단말기시험-가이드-010(03)
문서 제목	스마트폰 단독 단말기 시험 요구사항(2)
개정 이력	03 (개정), 2023년 6월 15일
적용 일자	2023년 6월 19일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

- [발행목적]

- 스마트폰 단독 신용카드 단말기의 운영환경 요구사항을 제시

- [적용범위]

- 스마트폰에 POS S/W에 해당하는 앱(App.)만 설치하고, 카드리더기는 별도로 부착하거나 연동하지 않고 스마트폰에 내재된 카메라나 NFC 기능을 사용하는 스마트폰 단독 단말기*

* 신용카드 단말기 정보보호 기술기준의 CAT단말기 또는 카드리더기로 간주

- [단말기시험-가이드-009와의 관계]

- 스마트폰 단독 단말기 인증을 위해서는 단말기시험-가이드-009 및 단말기시험-가이드-010을 모두 충족하여야 함

■ 세부가이드

- [스마트폰 단독 단말기 요구사항 및 제약사항]

- 스마트폰에 설치하는 앱(App.)과 신용카드 거래 처리 과정*은 정보보호산업진흥법에 따라 지정된 정보보호 전문서비스 기업 가운데 최소 2개 이상의 기업**으로부터 ①보안취약점 진단을 받고, ②발견된 취약점은 모두 조치되었다는 확인***을 받아야 함

* 스마트폰에 내재된 카메라와 NFC리더기가 읽은 민감한 신용카드 정보를 신용카드 거래 처리 과정에서 스마트폰의 모든 구성요소가 안전하게 다루는지 확인

** 단, 갱신시험의 경우 1개 이상의 기업

*** 보안취약점 진단을 모두 통과한 이후 해당 앱(App.)의 신용카드 거래 처리 과정은 임의변경 불가

o 앱(App.) 역공학 방지 기능* 및 최신 백신 프로그램 적용

* 난독화(ex 클래스, 메소드, 변수, 제어흐름, API 등), 암호화(ex 클래스, 문자열, 리소스 등) 및 동적 디버깅 방지 기능

o POS S/W에 해당하는 앱(App.)은 정식 앱스토어*에 등록되어야 함

* 안드로이드 : 구글 플레이스토어 / IOS : 앱스토어

o 앱(App.) UI/UX는 BIN 정보만을 표시*하고 화면 캡처를 방지해야 함

* 거래정보 확인을 위하여 일시적으로 마스킹된 카드번호(신용카드 번호 전체 자리 중 '9번째에서 12번째 번호와 가장 마지막 번호'를 *로 마스킹) 보기 기능 구현은 허용

단말기시험-가이드-011(00)-데몬형 POS 단말기 시험요구사항

문서 식별	단말기시험-가이드-011(00)
문서 제목	데몬형 POS 단말기 시험요구사항
개정 이력	00 (최초), 2019년 12월 26일
적용 일자	2019년 12월 26일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

- [발행목적]

- 다양한 형태의 데몬형 POS 단말기에 대한 일관된 기준을 제시함

- [적용범위]

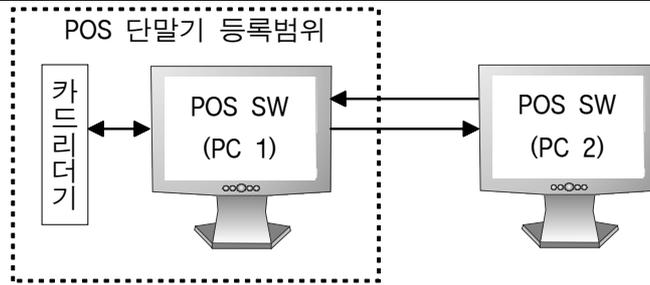
- 데몬형 형태의 POS 단말기(이하 '데몬형 POS 단말기')

- [용어정의]

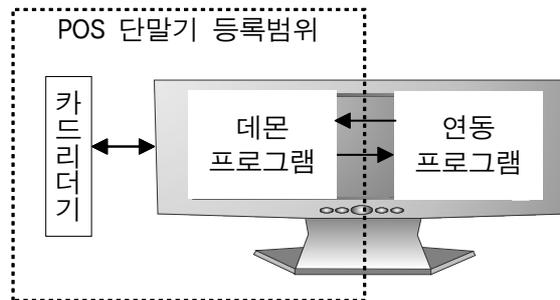
- 데몬형 POS 단말기 : 신용카드 결제를 위해 부가통신사업자(VAN)가 통제하는 'POS 소프트웨어'의 일부 기능이 백그라운드 형태로 동작하여 '연동 프로그램'에서 작업요청 시, POS 단말기의 기능을 수행하는 단말기
- 데몬 프로그램 : 신용카드 결제를 위해 부가통신사업자(VAN)가 통제하는 'POS 소프트웨어'의 일부 기능이 백그라운드 형태로 동작하도록 구현된 프로그램
- 연동 프로그램 : 데몬 프로그램과 연동하여 가맹점의 환경에 맞게 커스터마이징하여 구현된 프로그램

■ 세부가이드

데몬형 POS 단말기는 물리적으로 분리된 '인증대상 POS SW'와 '비 인증대상 POS SW(예: 가격정보를 송신하는 프로그램)'를 하나의 물리적인 단말기 내에서 동작하도록 구현한 형태의 구조를 가진다.



[그림 1] 외부 PC와 연동된 POS 단말기



[그림 2] 데몬형 POS 단말기

예로, 데몬형 POS 단말기는 그림 1과 같은 환경의 POS 단말기를 그림 2의 형태로 구현한 형태가 될 수 있다.

해당 단말기는 아래의 요구사항을 만족하여 구현하여야 하며, 요구사항을 만족하지 못하는 경우, 그림 2의 '연동 프로그램'도 'POS 단말기 등록범위'에 포함하여야 한다.

데몬 프로그램에서는 기본적으로 「신용카드단말기 정보보호 기술기준 (이하 '기술기준')」의 요구사항을 모두 만족해야 하며, 추가적으로 아래의 제약조건을 만족시켜야 한다.

- POS 단말기 내에서 '민감한 신용카드 정보' 및 '신용카드번호'는 저장할 수 없다.
- 데몬 프로그램에서 연동 프로그램으로 '민감한 신용카드 정보' 및 '신용카드번호'를 전송할 수 없다(마스킹된 신용카드 번호, 암호화된 데이터 포함).

※ 단, 신용카드번호 앞 6자리 정보는 송신 가능

- 마스킹된 신용카드 번호는 데몬 프로그램에서 출력은 가능하나 사용 즉시 삭제해야 한다.
 - ※ 단, 신용카드번호 앞 6자리 정보는 저장 가능
- 기술기준 '5.4 신용카드 번호 보호'에 해당하는 신용카드번호는 평문형태로 전송이 불가(전용선 포함)하며, 암호화된 경우 전송 구간에서(단말기→VAN사 서버) 복호화 되지 않아야 한다(중계서버 등에서 복호화 불가).
- 키인 거래 시, 카드리더기에서 입력 및 암호화가 수행되어야 한다.
- 데몬 프로그램이 카드 매출전표 출력을 통제한다면 기술기준 제4절 '7. 카드 매출전표 출력에 대한 요구사항'을 만족해야 한다.
- 데몬 프로그램과 연동 프로그램 사이에 송·수신 되는 정보는 문서로 시험기관에 제출하여야 한다.

단말기시험-가이드-012(00)-면세점용 신용카드 단말기

문서 식별	단말기시험-가이드-012(00)
문서 제목	면세점용 신용카드 단말기
개정 이력	00 (최초), 2020년 10월 21일
적용 일자	2020년 11월 2일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

- [발행목적]

- 면세점에서 사용하는 신용카드 단말기에서 액체, 젤류 및 에어로졸 제품을 판매하는 경우 카드 매출전표 출력에 대한 기준 안내

- [적용범위]

- 면세점에서 사용하는 신용카드 단말기

■ 세부가이드

면세점에서 사용하는 신용카드 단말기에서 액체, 젤류 및 에어로졸 제품을 포함하여 판매하는 경우 회원용 카드 매출전표를 회원 의사와 무관하게 발급 가능하도록 기능 구현 가능

※ 단, 액체, 젤류 및 에어로졸 이외 제품만 판매시 회원 의사에 따라 선택 발급 적용 필수

단말기시험-가이드-013(00)-POS 단말기 POS-ID 부여 시험요구사항

문서 식별	단말기시험-가이드-013(00)
문서 제목	POS 단말기 POS-ID 부여 시험요구사항
개정 이력	00 (최초), 2020년 12월 15일
적용 일자	(최초시험)2021년 1월 4일 / (변경시험)2021년 4월 1일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

- [발행목적]

- POS 단말기에 등록된 POS S/W 설치(AS 등을 위한 재설치 포함)시 부가통신업자(VAN사)가 해당 POS 단말기에 고유번호를 부여하고, POS 단말기에서 발생하는 승인/승인취소 요청 전문에 동 고유번호를 반영하기 위한 시험 요구사항을 제시

- [적용범위]

- POS 단말기(POS S/W)

※ 단, 인증서보유기관이 가맹점 등으로서 카드 매출을 직접 관리 하는 등 VAN사가 고유번호를 부여하기 어려운 경우 인증서보유기관이 예외 처리 요청 공문을 시험업무 수탁기관에 제출하면 적용 제외 가능하고, 이 경우 단말기식별번호 13번째 byte를 'Z'로 표기

■ 세부가이드

POS S/W 설치시 VAN사가 해당 POS 단말기를 고유하게 관리 할 수 있도록 POS-ID를 부여하고, POS 단말기 내부에 안전하게 보관 되도록 구현

o 상세 요구사항

- ① POS-ID(고유번호) 는 VAN사가 부여
- ② 부여된 POS-ID(고유번호)는 POS 단말기에서 안전하게 보관(인코딩 처리 등)
- ③ 승인/승인취소 요청 전문에 POS-ID(고유번호) 반영
- ④ 자체 매출 관리 등 가맹점 특성에 따라 상기 요구사항을 비활성화 할 수 있는 기능 구현 가능

※ 단, 특정 POS S/W가 2개 이상의 VAN사를 지원하는 경우 주 VAN사가 부여한 POS-ID 공유 가능

단말기시험-가이드-014(00)-8자리 BIN 체계 시험요구사항

문서 식별	단말기시험-가이드-014(00)
문서 제목	8자리 BIN 체계 시험요구사항
개정 이력	00 (최초), 2021년 11월 29일
적용 일자	(최초시험)2022년 4월 1일 (변경시험)2022년 7월 1일 (갱신시험)2023년 4월 1일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

- [발행목적]

- 8자리 BIN 체계 도입에 따라 ①신용카드 회원/가맹점간 커뮤니케이션 혼선 방지, ②카드 결제시 발급사 오분류에 따른 승인 오류 방지를 위해 단계적으로 8자리 BIN 처리 기준 활용 의무화

- [적용범위]

- CAT/POS 단말기

■ 세부가이드

CAT/POS단말기가 매입 업무처리, 제휴서비스 연계, 매출전표 출력 등을 위하여 신용 카드정보 리딩시 8자리 BIN 기준으로 처리 되도록 구현

o 상세 요구사항

구분	상세내용
발급사 분류	카드번호 16자리 중 앞에서부터 8자리를 BIN으로 인식
마스킹 처리	카드번호 9~12번째와 마지막 번호 마스킹

- 「신용카드 단말기 정보보호 기술기준」에 명시된 '7번째에서 12번째 번호' 마스킹 기준은 동 시험가이드의 단계별 적용 일자 이후 사용 불가
- '데몬형 POS 단말기 시험요구사항(문서식별 : 단말기시험-가이드-011(00))'에 명시된 전송가능 신용카드번호도 상기 적용 일자에 따라 앞에서부터 8자리만 전송 가능

단말기시험-가이드-015(00)-비접촉식 결제전용 장치 등 연동 시험요구사항

문서 식별	단말기시험-가이드-015(00)
문서 제목	비접촉식 결제전용 장치 등 연동 시험요구사항
개정 이력	00 (최초), 2023년 8월 1일
적용 일자	2023년 8월 14일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

• [발행목적]

- 비접촉식 결제 수용을 위하여 신용카드 단말기에 비접촉식 결제 전용 장치 또는 비접촉식 결제전용 카드리더기를 연동하는 경우 준수해야할 세부 요구사항을 제시

• [적용범위]

- 비접촉식 결제전용 장치 또는 비접촉식 결제전용 카드리더기를 연동하여 비접촉식 결제를 수용하는 신용카드 단말기

• [용어정의]

- “비접촉식 결제전용 장치”라 함은 NFC 통신을 통해 비접촉식 카드 (모바일, 웨어러블 등 Card Emulation을 포함한다) 결제를 수용할 수 있는 장치로 독립적인 보안기능(신용카드 단말기 정보보호 기술 기준을 만족하는 보안 요구사항)을 수행하지 않는 장치를 의미한다. 단, 결제 어플리케이션 또는 커널 등이 탑재되지 않은 NFC 리더기와 같이 비접촉식 거래를 단독으로 수행하지 못하는 장치는 해당되지 않는다.
- “비접촉식 결제전용 카드리더기”라 함은 NFC 통신을 통해 비접촉식 카드(모바일, 웨어러블 등 Card Emulation을 포함한다) 결제를 수용할 수 있는 장치로 독립적인 보안기능(신용카드 단말기 정보보호 기술 기준을 만족하는 보안 요구사항)을 수행하는 장치를 의미한다.
- “물리적 결합”이라 함은 장치간 기구 결합(나사, 스냅핏, 리벳 등) 또는 시건장치 등에 의해 신용카드 단말기와 비접촉식 결제전용 장치가 결합되어 하드웨어에 대한 접근을 통제할 수 있으며, 물리적인 전용선을 통해 장치간 통신을 수행하는 구조*를 말한다.

* 기구 결합 또는 시건장치 등 없이 단순 케이블을 통한 연결은 물리적 결합이라 보지 않음

• [단말기시험-가이드-001 및 006과의 관계]

- '사용 시간과 사용 횟수에 제한이 동시에 있는 일회용 토큰' 및 '사용 시간과 사용 횟수에 제한이 없는 고정형 토큰' 만을 수용하는 비접촉식 전용 단말기는 본 시험요구사항을 적용받지 않는다.

■ 세부가이드

비접촉식 결제전용 장치 및 카드리더기 연동 방식별 시험 허용 기준

단말기 유형	연동 장치	
	비접촉식 결제전용 카드리더기	비접촉식 결제전용 장치
POS 단말기	허용	불허
CAT 단말기	허용	허용
카드리더기	불허	허용(물리적 결합 구조를 통한 연동 限)

비접촉식 결제전용 카드리더기에 대한 시험 요구사항

- 비접촉식 결제전용 카드리더기는 신용카드 단말기 정보보호 기술기준 및 단말기 시험 가이드상 카드리더기에 대한 요구사항을 준수해야하며, 카드리더기로 등록되어야 함

비접촉식 결제전용 장치는 다음과 같은 시험요구사항을 만족해야 한다.

연동 방식		세부 요구사항
[CAT 단말기]	1. 물리적 결합 구조를 통해 연동	① 비접촉식 결제전용 장치와 CAT 단말기는 특정 장치와만 연결될 수 있도록 상호인증 메커니즘을 구현해야 함 ② 비접촉식 결제전용 장치와 CAT 단말기 사이의 통신구간은 암호화 또는 보안 통신 채널 수립 등의 방식으로 보호되어야 함(※ 단, 하나의 제품으로 취급할 수 있을 정도의 물리적 결합을 통해 비인가 접근통제가 가능한 구조를 갖춘 경우는 제외) ③ 비접촉식 결제전용 장치는 CAT 단말기와 함께 등록되어야 함 ④ 비접촉식 결제전용 장치와 CAT 단말기 연동에 사용되는 모든 정보는 문서로 시험기관에 제출되어야 함

		⑤ 비접촉식 결제전용 장치가 CAT 단말기에 연동된 경우에는 별도의 식별번호를 부여해야 하며, 이 식별번호는 비접촉식 결제전용 장치와 CAT 단말기 간 상호인증 과정에서 설정되어야 함
	2. 물리적 결합이 아닌 구조를 통해 연동*	① CAT 단말기와 물리적으로 결합되지 않는 비접촉식 결제전용 장치는 비접촉식 결제전용 카드리더기로 간주하여, 신용카드 단말기 정보보호 기술기준 및 단말기 시험 가이드상 카드리더기에 대한 요구사항을 준수해야하며, 카드리더기로 등록되어야 함
[카드리더기]	1. 물리적 결합 구조를 통해 연동	① 비접촉식 결제전용 장치와 카드리더기는 특정 장치외만 연결될 수 있도록 상호인증 메커니즘을 구현해야 함 ② 비접촉식 결제전용 장치와 카드리더기 사이의 통신구간은 암호화 또는 보안 통신 채널 수립 등의 방식으로 보호되어야 함(※단, 하나의 제품으로 취급할 수 있을 정도의 물리적 결합을 통해 비인가 접근통제가 가능한 구조를 갖춘 경우는 제외) ③ 비접촉식 결제전용 장치는 카드리더기와 함께 등록되어야 함 ④ 비접촉식 결제전용 장치와 카드리더기 연동에 사용되는 모든 정보는 문서로 시험기관에 제출되어야 함 ⑤ 비접촉식 결제전용 장치가 카드리더기에 연동된 경우에는 별도의 식별번호를 부여해야 하며, 이 식별번호는 비접촉식 결제전용 장치와 카드리더기 간 상호인증 과정에서 설정되어야 함
	2. 물리적 결합이 아닌 구조를 통해 연동*	① 카드리더기와 물리적으로 결합되지 않는 비접촉식 결제전용 장치 또는 비접촉식 결제전용 카드리더기의 연동은 허용되지 않음

* ex. 물리적인 전용선 연결형태만 사용하는 경우

- 비접촉식 결제전용 장치는 연동되는 CAT 단말기 또는 카드리더기와 함께 시험기관에 제출되어야 하며, 다른 신용카드 단말기와 연동될 수 없음

비접촉식 결제전용 장치가 연동된 신용카드 단말기의 등록 범위를 아래와 같이 적용

구분	단말기 등록 범위				
	단말기 외관	단말기 HW	전용장치 외관	전용장치 HW	연동된 외관
CAT 단말기	대상	대상	대상	대상	대상
카드리더기	대상	대상	대상	대상	대상

단말기시험-가이드-016(00)-POS 소프트웨어 운영환경 시험요구사항

문서 식별	단말기시험-가이드-016(00)
문서 제목	POS 소프트웨어 운영환경 시험요구사항
개정 이력	00 (최초), 2023년 6월 15일
적용 일자	2023년 6월 19일
공개 범위	<input checked="" type="checkbox"/> 인증기관 <input checked="" type="checkbox"/> 시험기관/시험업무 수탁기관 <input checked="" type="checkbox"/> 신청기관

■ 문서개요

- [발행목적]
 - 범용 운영체제에서 동작되는 POS 소프트웨어의 운영환경 요구사항을 제시
- [적용범위]
 - 운영체제가 범용 OS(예: Windows, Mac, Android, iOS)인 단말기

■ 세부가이드

PC 기반의 범용 운영체제에서 동작되는 신용카드 단말기는 다음과 같은 시험 요구사항을 만족해야 한다.

- [운영환경 보안-01] 보안패치가 이루어지는 범용 운영체제 버전을 사용해야 한다.

모바일 기반의 범용 운영체제에서 동작되는 신용카드 단말기는 다음과 같은 시험 요구사항을 만족해야 한다.

- [운영환경 보안-02] 보안패치가 이루어지는 범용 운영체제 버전을 사용해야 한다.
- [운영환경 보안-03] 제조사의 보안 업데이트가 이루어지는 모바일 기기를 사용해야 한다.

시험 신청 유형에 따라 운영환경 보안 요구사항을 아래와 같이 적용

구분	시험 신청 유형			
	최초시험/재시험	변경시험	갱신시험	사용연장
운영환경 보안 요구사항 적용	대상	대상	대상	비대상*

- * 단, 사용연장 신청시 사용 중인 POS 소프트웨어의 운영환경에 대해 기술 필요
- ※ 신청기관은 위의 요구사항을 만족하는 신용카드 단말기를 시험기관에 제출해야 한다.