신용카드 회원의 정보보호를 위한

신용카드 단말기 정보보호 기술기준

2018. 1. 25

여 신 금 융 협 회

목 차

제1장 개요

제1절 목적

본 문서는 『여신전문금융업법 제27조의4(신용카드 단말기의 등록)②』 및 『동법 시행령 제7조의6(신용카드 단말기 등록요건 등)①』에 따라 부가통신업자가 전기통신서비스를 제공하는 신용카드 단말기를 금융위원회에 등록(또는 부가통신업자가 전기통신서비스를 제공하지 아니하는 신용카드 단말기의 경우에는 신용카드가맹점이 금융위원회에 등록)하기 위해 신용카드 단말기가 갖추어야 하는 정보보호 기술기준을 제시하는 것을 목적으로 한다.

제2절 적용범위

적용범위

o **대상제품** : 금융위원회에 등록하고자 하는 신용카드 단말기
- 관련 유형 : 신용카드 단말기 시험·인증 및 등록관리규정 제2조 제1항에 따른 신용카드 단말기로서, CAT단말기와 POS단말기로 구분. 단, 민감한 신용카드 정보를 이용하지 않는 장치는 신용카드 단말기 정보보호 기술기준 적용 대상에서 제외

o **적용대상 서비스** : 신용카드 단말기를 통한 거래승인 결제 서비스

『여신전문금융업법 제27조의4(신용카드 단말기의 등록)① 및 ②』에 따라 신용카드회원 정보보호를 위한 안전한 신용카드 단말기 등록·운영 지원체계는 다음과 같다.

<표 1> 기관별 역할

구분	기관명	주요내용
정책기관	금융위원회	▪ 신용카드 단말기 정보보호 관련 제도 마련 및 정책 수립 ▪ 신용카드 단말기 등록·관리 지침 고시
위탁기관	여신금융협회	▪ 신용카드 단말기 등록 및 기술기준에 관한 업무 - 신용카드 단말기 등록·관리절차 마련 및 시행 ▪ 신용카드 단말기 정보보호 기술기준 시험기관 및 인증기관 업무 - 신용카드 단말기 정보보호 기술기준에 따른 시험 및 성적서 발급 - 신용카드 단말기 정보보호 시험결과 인증 및 인증서 발급
의뢰기관	부가통신업자, 카드리더기 제조업체 등 신용카드 단말기 개발 및 운영주체	▪ 신용카드 단말기 정보보호 기술기준에 따른 제품 개발 ▪ 보안약점(및 보안취약점) 점검 및 보완조치
사용기관	신용카드가맹점 등	▪ 금융위원회에 등록된 안전한 신용카드 단말기 구축·운영

제3절 관련 법령 및 규정

신용카드 단말기 정보보호와 관련된 법률 및 규정은 다음과 같다.

1. 법령

1) 여신전문금융업법(2015.7.21., 법률 제13068호)

제4절 문서구성

본 문서는 다음의 3개장과 부록으로 구성된다.

- 1장 : 문서의 목적 및 적용범위, 용어정의 설명
- 2장 : 신용카드 단말기 구성 및 주요 보안위협 내용 설명
- 3장 : 신용카드 단말기에 요구되는 정보보호 요구사항 내용 설명
- 부록 : 신용카드 단말기 유형별 보안기능 및 시험요구사항 내용 설명

제5절 용어정의

본 문서에서 사용하는 용어의 정의는 다음과 같으며, 그 이외 용어는 관련 법령 및 규정에 따른다.

1. "**신용카드**"는 이를 제시함으로써 반복하여 신용카드가맹점에서 『여신전문금융업법』 제2조(정의) 제3항의 각 목(가~라)을 제외한 사항을 결제할 수 있는 증표(證票)로서 신용카드업자(외국에서 신용카드업에 상당하는 영업을 영위하는 자를 포함한다)가 발행한 것이다. 본 문서에서 말하는 신용카드는 체크카드와 선불카드(기프트카드)를 포함한다.

2. "**신용카드 정보**"란 신용카드 전자거래를 위해 신용카드 마그네틱선 또는 IC 칩 등에 전자적으로 존재하는 신용카드 번호, 유효기한, 소유주 이름, 신용카드 유효성 검증값 등을 말하며, 일부 정보는 신용카드 겉면에서 육안으로 식별 가능하다.

3. "**신용카드 거래정보**"란 신용카드 거래승인 요청 시 신용카드업체에서 전송하는 카드번호, 유효기한, 승인금액, 승인번호, 승인일자, 가맹점번호, 할부기간을 말한다.

4. "**민감한 신용카드 정보**"란 외부 유출시 신용카드 회원에게 금전적 손실을 발생시킬 수 있는 중요 정보로 신용카드 번호, 유효기한, 신용카드 유효성 검증값, PIN(Personal Identification Number) 유효성 검증값 등이 이에 해당된다.
   ※ 사용 시간과 사용 횟수에 제한이 있는 형태의 신용카드 번호 등은 민감한 신용카드 정보로 분류되지 않는다.

5. "**신용카드 유효성 검증값**"이란 CVC/CVV/CAV/CSC* 등 신용카드 부정사용 예방을 목적으로 거래승인 시 검증되는 신용카드사 고유의 검증값을 말한다.
   * CVC : Card Validation Code, CVV : Card Verification Value, CAV : Card Authentication Value, CSC : Card Security Code

6. “**PIN 유효성 검증값**”이란 PVV, PVKI* 등 신용카드 부정사용 예방을 목적으로 거래승인 시 검증되는 값을 말한다.

* PVV : PIN Verification Value, PVKI : PIN Verification Key Indicator

7. “**신용카드 매출전표**”란 신용카드 거래에 대하여 신용카드업체로부터 정상승인 응답을 수신 받은 경우 출력되는 증빙자료 말한다.

8. “**CAT(Credit Authorization Terminal) 단말기**”란 신용카드가맹점 등에서 신용카드 등의 거래승인을 위해 사용되는 발행회사, 회원번호 등을 자동 판독해 통신회선을 통하여 신용카드업체로 전달하고 정산해주는 일반 결제 단말기를 말한다.

9. “**POS(Point of Sale) 단말기**”란 신용카드가맹점에 설치되어 판매상품조회, 매출조회 등 다양한 판매시점 관리기능과 신용카드에 의한 거래발생 건에 대하여 신용카드업체로부터 거래승인을 받기 위하여 거래승인 기능을 제공하는 단말 장치를 말하며, POS 단말기 본체(PC 또는 전용 하드웨어)와 카드리더기로 구성된다. POS 단말기 본체와 카드리더기는 유·무선으로 연결되거나 카드리더기가 POS 단말기 본체에 내장될 수 있다.

10. “**카드리더기(Card Reader)**”란 신용카드 거래를 발생시키기 위해 필요한 정보를 읽을 수 있는 기능을 제공하는 다양한 형태의 기계장치를 말한다.

11. “**부가통신업자(Value Added Network,** 이하 ‘VAN’이라 한다)”란 신용카드업자 및 신용카드가맹점과의 계약에 따라 단말기 설치, 신용카드 등의 조회·승인 및 매출전표 매입·자금정산 등 신용카드 등의 대금결제를 승인·중계하기 위한 전기통신서비스 제공하는 업체로 금융위원회에 등록한 업체를 말한다.

12. “**암호키**”란 거래승인과 관련된 민감한 신용카드 정보를 암호화하기 위하여 사용되는 키를 말한다.

13. “**단말기시험 가이드**”란 기술기준의 정보보호 요구사항, 보안기능 및 시험요구사항을 명확하게 해석하여 적용하고, 최신 보안취약점을 조치하기 위해 인증기관이 별도로 발행한 보조문서를 말한다.

제2장 신용카드 단말기 구성 및 주요 보안위협

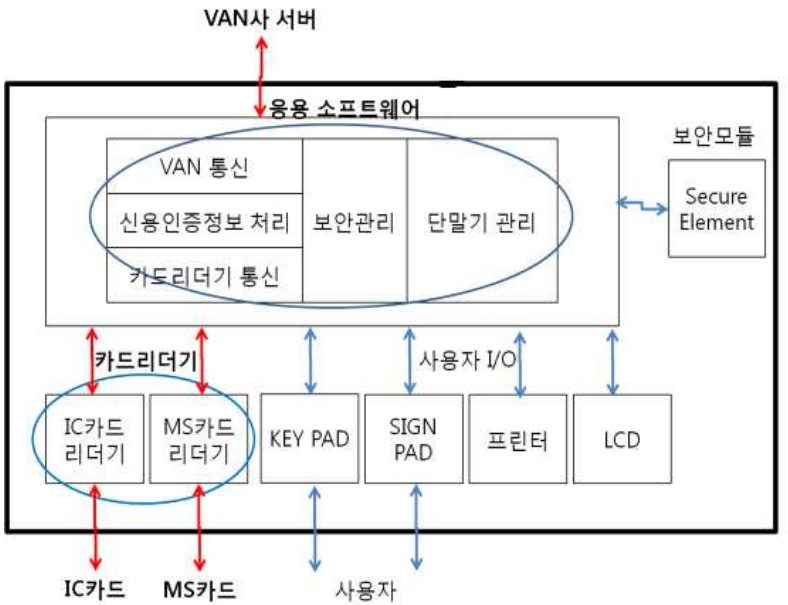
신용카드 단말기 유형에 따른 구성과 신용카드 단말기에 대한 주요 보안위협을 소개한다.

제1절 신용카드 단말기 구성

신용카드 단말기 유형은 CAT 단말기와 POS 단말기 등으로 구분할 수 있으며 각각에 대한 주요 기능과 운영환경에 대해 설명한다.

1. CAT 단말기

CAT 단말기는 신용카드 등의 거래승인을 위해 카드리더기로 부터 입력된 민감한 신용카드 정보를 VAN으로 전달하는 신용지불 단말장치로 일반적으로 단독으로 운영하며 필요시 POS 단말기와 연동하여 사용할 수 있다. 일반적인 CAT 단말기 구조는 [그림 1]과 같다.

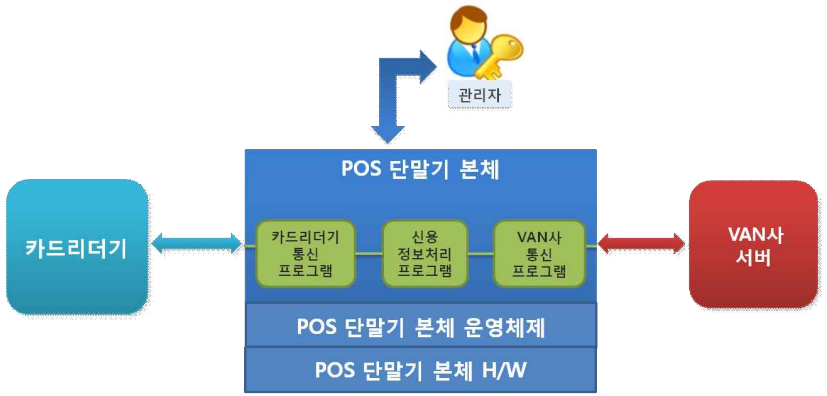


[그림 1] 일반적인 CAT 단말기 구조

2. POS 단말기

POS 단말기는 신용카드가맹점에 설치되어 판매상품조회, 매출조회 등 다양한 판매시점 관리기능과 신용카드에 의한 거래발생 건에 대하여 신용카드업체로부터 거래승인을 받기 위하여 거래승인기능을 제공하는 단말장치로 신용카드 결제기능 이외에 현금결제, 상품권 결제 등 다양한 금융결제기능과 관련된 금융정보를 취급할 수 있다.

POS 단말기는 물리적으로 일반 PC 또는 POS 전용 단말기 하드웨어 등의 POS 단말기 본체와 카드리더기로 구성되며 POS 단말기 본체와 카드리더기는 유·무선으로 연결되거나 카드리더기가 POS 단말기 본체에 내장될 수 있다. 일반적인 POS 단말기 구조 및 구성환경은 다음과 같다.



[그림 2] 일반적인 POS 단말기 구조 및 구성환경

제2절 주요 보안위협

신용카드 단말기와 관련된 주요 보안위협은 다음과 같다.

<표 2> 주요 보안위협

보안위협	설명	주요 보안 대책
중요정보 불법접근	메모리 해킹, 탭핑, 스키밍, 악성코드 등의 공격 기법*을 사용하여 중요정보(민감한 신용카드 정보, 신용카드 번호)을 유출할 수 있는 보안위협	·중요정보 암호화
암호키 유출	중요정보 암호화 연산을 위해 사용되는 암호키가 유출되어 중요정보가 유출될 수 있는 보안위협	·안전한 암호키 관리
전송데이터 유출	신용카드 단말기 구성요소간 또는 신용카드 단말기와 VAN 서버간 전송되는 중요정보를 무단으로 노출, 변경시킬 수 있는 보안위협	·암호화 통신 제공
보안기능 우회	악성코드를 통해 신용카드 단말기 보안기능과 관련된 실행파일 또는 설정파일 등이 변조되어 보안기능을 우회할 수 있는 보안위협	·자체보호 기능 ·안티바이러스 제품 설치·운영

* 주요 공격기법에 대한 설명은 다음과 같다.

<표 3> 주요 공격기법

공격기법	설명
메모리 해킹	이용자가 입력한 데이터 등이 메모리상에 평문으로 처리되는 구간을 포착하여 민감한 신용카드 정보, 신용카드 번호, 암호키를 추출해 내는 공격기법
스키밍(Skimming)	카드입력부(예, 카드리더기) 등에 부착되어 민감한 신용카드 정보 등을 빼내어 카드 정보를 전자적으로 복제하는 공격기법
탭핑(Tapping)	카드입력부(예, 카드리더기)와 신용카드 단말기 사이의 케이블을 도청하여 민감한 신용카드 정보 등을 절취하고 복제하는 공격기법

제3장 신용카드 단말기 정보보호 요구사항

제1절 개요

본 문서에서 고려하는 신용카드 단말기의 보안성 수준은 '강화된 기본' 수준의 공격 성공 가능성을 지닌 공격을 방어하는 수준의 보안기능 구현이다. 이에 따른 신용카드회원의 정보보호를 위해 신용카드 단말기 개발 시 구현해야 하는 기본 요구사항 및 기술적 요구사항과 신용카드 단말기에 대한 안전한 구축 운영을 위한 관리적 요구사항을 설명한다. 다음은 각 요구사항에 대한 요약 설명이다.

<표 4> 신용카드 단말기 정보보호 기술기준 요약

구분	정보보호 요구사항	세부항목
기본 요구사항 (제2절)	신용카드 거래승인에 대한 요구사항	2개 항목
	신용카드 처리에 대한 요구사항	2개 항목
기술적 요구사항 (제3절)	민감한 신용카드 정보에 대한 보안요구사항	3개 항목
	신용카드 정보에 대한 보안요구사항	5개 항목
	암호화에 대한 보안요구사항	4개 항목
	자체보호에 대한 보안요구사항	3개 항목
관리적 요구사항 (제4절)	안전한 소프트웨어 개발에 대한 요구사항	1개 항목
	초기 암호키 주입에 대한 요구사항	2개 항목
	보안교육에 대한 요구사항	1개 항목
	형상관리에 대한 요구사항	3개 항목
	안전한 운영환경 구성에 대한 요구사항	4개 항목
	보안취약점 점검 및 조치에 대한 요구사항	2개 항목

인증기관은 본 문서에 서술된 정보보호 요구사항(기본 요구사항, 기술적 요구사항, 관리적 요구사항)과 부록(CAT 단말기 보안기능 및 시험요구사항, POS 단말기 보안기능 및 시험요구사항)에 서술된 각 요구사항을 명확하게 해석하여 적용하고, 최신 보안취약점 조치를 위해 "단말기시험 가이드"를 별도로 발행할 수 있다.

제2절 기본 요구사항

신용카드 단말기로 정상적인 신용카드 거래를 하기 위한 기본 요구사항은 다음과 같다.

1. 신용카드 거래승인에 대한 요구사항

신용카드 회원의 정보보호를 위해 안전한 유형의 신용카드를 우선 사용하도록 다음 요구사항을 만족해야 한다.

1.1 신용카드 단말기는 ISO7816에서 규정한 ID-1 TYPE 형태의 카드가 이용되는 경우 EMV(Europay Mastercard Visa) 거래 또는 이에 준하는 방식으로 우선 처리함을 원칙으로 한다.

1.2 비정상적 fall-back 거래 및 변칙적 MS 거래가 발생하지 않도록 해야 한다.

2. 신용카드 처리에 대한 요구사항

신용카드 단말기가 다양한 신용카드에 대한 거래를 처리할 수 있도록 보장하기 위해 다음과 같은 요구사항을 만족해야 한다.

2.1 국내에서 발급되는 모든 종류의 신용카드를 수용하여야 처리할 수 있어야 한다.

2.2 신용카드 단말기에 대한 안전성 및 호환성을 보장해야 한다.

제3절 기술적 요구사항

신용카드 회원 정보를 보호하기 위한 신용카드 단말기의 기술적 보안 요구사항은 다음과 같다.

1. 민감한 신용카드 정보에 대한 보안요구사항

신용카드 거래를 위해 필요한 민감한 신용카드 정보를 보호하기 위해 다음 요구사항을 만족해야 한다.

1.1 신용카드로부터 입력받은 민감한 신용카드 정보는 암호화하여 전송 및 처리해야 하며, 평문상태로 존재하지 않아야 한다.

1.2 민감한 신용카드 정보는 어떠한 형태로도 메모리 및 파일시스템에 저장되지 않아야 한다.

1.3 민감한 신용카드 정보는 신용카드 매출전표 및 단말기 화면에 출력되지 않아야 한다.

2. 신용카드 정보에 대한 보안요구사항

신용카드업체가 승인한 매입 업무처리, 신용카드업체 제휴서비스 연계, 신용카드 매출전표 출력의 목적으로 신용카드 정보가 필요한 경우, 민감한 신용카드 정보 보호와 별도로 신용카드 번호 보호를 위해 다음과 같은 요구사항을 만족해야 한다.

2.1 신용카드로부터 입력받은 신용카드 정보는 암호화 또는 마스킹(신용카드 번호 16자리 중 7번째에서 12번째 번호를 '*'로 마스킹)하여 전송하거나, 전용망을 이용한 전송 등의 방법을 통해 안전하게 전송되어 처리되어야 한다.

2.2 신용카드 정보는 암호화 또는 마스킹하거나, 거래를 구분할 수 있는 다른 정보 등으로 변환되어 안전하게 저장되어야 한다.

2.3 안전하게 저장되어 관리되고 있는 신용카드 정보는 최대 3개월 이내에 삭제되어야 한다.

2.4 신용카드 거래승인이 완료된 경우, 거래 종료시점에 신용카드 번호가 가용하지 않도록 메모리에서 삭제해야 한다.

2.5 신용카드 번호를 신용카드 단말기 화면 또는 신용카드 매출전표에 출력하는 경우 마스킹(신용카드 번호 16자리 중 7번째에서 12번째 번호를 '*'로 마스킹)된 정보가 표시되어야 한다.

3. 암호화에 대한 보안요구사항

민감한 신용카드 정보 및 신용카드 번호 암호화를 위한 안전한 암호화 연산 및 암호키 관리(생성, 분배, 폐기)를 위해 다음 요구사항을 만족해야 한다.

3.1 암호화 연산은 112비트 이상의 보안강도를 갖는 암호알고리즘과 암호키 길이에 따라 암호화 되어야 한다.

3.2 안전성이 검증된 암호키 생성 및 분배 방법이 사용되어야 한다.

3.3 사용이 만료·종료된 암호키 및 암호키 생성·분배를 위해 사용된 모든 정보는 카드리더기를 포함한 신용카드 단말기에서 파기 및 삭제되어야 한다.

3.4 암호화된 민감한 신용카드 정보 또는 신용카드 번호를 임의로 복호화 할 수 없도록 암호키가 유출되지 않는 안전한 암호키 관리 메커니즘을 구현해야 한다.

4. 자체보호에 대한 보안요구사항

신용카드 단말기의 정상적인 동작을 보장하기 위해 다음과 같은 요구사항을 만족해야 한다.

4.1 신용카드 단말기 시동 및 운영(주기적 또는 관리자 요청)시 보안기능 실행코드 및 보안기능 관련 저장데이터(보안기능 관련 프로그램 설정값 등) 변경 여부를 탐지하기 위한 무결성 점검 기능을 제공해야 한다.

4.2 무결성 점검 수행결과를 관리자가 조회할 수 있는 기능을 제공해야 한다.

4.3 무결성 검증 실패에 대한 대응행동(동작 중단 및 관리자에게 통보)을 제공해야 한다.

제4절 관리적 요구사항

신용카드 회원 정보를 보호하기 위한 신용카드 단말기 개발 및 운영에 대한 관리적 요구사항은 다음과 같다.

1. 안전한 소프트웨어 개발에 대한 요구사항

안전한 신용카드 단말기의 개발을 위해 다음과 같이 소프트웨어 개발보안을 적용하여 개발할 것을 권고한다.

1.1 안전한 신용카드 단말기 프로그램 개발을 위해 개발단계부터 취약점의 원인을 배제하도록 소프트웨어 개발보안 방법론을 채택하여 개발해야 한다.

2. 초기 암호키 주입에 대한 요구사항

민감한 신용카드 정보 및 신용카드 번호 암호화를 위해 사용되는 암호키를 생성하기 위한 초기 암호키를 안전하게 신용카드 단말기에 주입하여 배포할 수 있도록 다음과 같은 관리대책을 마련하여 시행하는 것이 필요하다.

2.1 신용카드 단말기 제조직후 주입되는 초기 암호키는 안전하게 관리되어야 한다.

2.2 신용카드 단말기에 초기 암호키 주입 시 인가된 직원이 안전한 장소에서, 안전한 방법으로 초기 암호키를 주입할 수 있도록 관리되어야 한다.

3. 보안교육에 대한 요구사항

신용카드가맹점 등과 같은 수요처에 신용카드 단말기를 제공한 VAN 등과 같은 기관은 신용카드 단말기가 안전하게 구축·운영될 수 있도록 다음과 같이 보안교육을 수행할 것을 권고한다.

3.1 신용카드 단말기를 안전하게 구축·운영할 수 있도록 관리자 및 사용자에 대한 운영 관련 보안교육 계획을 수립하여 주기적으로 수행해야 한다.

4. 형상관리에 대한 요구사항

신뢰할 수 있는 신용카드 단말기 서비스 환경을 제공하기 위하여 다음과 같이 형상관리 체계를 도입하여 운영 및 관리하는 것이 필요하다.

4.1 신용카드 단말기 개발 시 형상관리 체계를 수립하고 형상관리 계획에 따라 운영 및 관리하여야 한다.

4.2 형상관리 체계에서 모든 형상항목은 유일하게 식별되어야 한다.

4.3 형상항목의 변경은 인가된 변경만 허용해야 하며 변경사항은 추적되어야 한다.

5. 안전한 운영환경 구성에 대한 요구사항

안전한 신용카드 단말기 서비스 제공을 위해 다음과 같이 안전한 운영환경을 구축하는 것이 필요하다.

5.1 신용카드 단말기가 일반 범용 운영체제에서 동작할 경우, 시스템 제공 및 관리 업체에서 운영체제의 기본 보안 설정을 구성해야 한다.

5.2 운영체제, 방화벽, 안티바이러스 제품 등에 대해 필수 보안패치를 적용할 수 있는 관리 수단을 제공해야 한다.

5.3 신용카드 단말기 관련 소프트웨어(카드리더기통신/신용인증정보처리/VAN통신프로그램) 및 원격제어 소프트웨어 등의 프로그램 이용 및 설치 시 신뢰할 수 있는 특정 구간의 IP 주소, 포트(Port), 프로토콜(Protocol) 등만 허용하도록 설정되어야 한다.

5.4 신용카드 결제기능을 위한 신규 환경 구성, 단말기 A/S에 의한 결제기능 환경 재구성 등으로 인하여 CAT-ID를 설정하여야 하는 경우 반드시 VAN으로부터 CAT-ID 번호를 검증받아 설정하여야 한다.

6. 보안취약점 점검 및 조치에 대한 요구사항

신용카드 단말기를 제공한 VAN 등은 안전한 신용카드 결제서비스 제공을 위해 다음과 같이 주기적으로 신용카드 단말기 프로그램 및 운영환경에 대한 보안취약점을 점검하여 조치를 취해야 한다.

6.1 신용카드 단말기 프로그램에서 보안취약점 발견 시 보안취약점을 조치하여 보안패치를 먼저 배포하고 시험기관에 보안패치 프로그램에 대한 시험을 의뢰해야 한다.

6.2 신용카드 단말기 운영환경에 대한 보안취약점 발견 시 신용카드 단말기가 설치된 신용카드가맹점 등에 해당 내용을 공지하여 보안패치를 적용할 수 있도록 해야 한다.

[별표] 신용카드 단말기 정보보호 기술기준과 시험요구사항간 연관관계

구분	정보보호 요구사항	기술기준	CAT단말기(부록1)	POS단말기(부록2)
기본 요구사항 (제2절)	1. 신용카드 거래승인	1.1	4.1.1 IC우선거래	
			4.2.1 신용카드 거래의 안전성 및 호환성 보장	
		1.2	4.1.1 비정상적 fall-back 거래	
			4.1.1 변칙적 MS거래	
	2. 신용카드 처리	2.1	4.3.1 국내 발급 모든 신용카드 수용	
			4.4.1 선불카드(기프트카드) 잔액 표시	
		2.2	5. 시험요구사항	
기술적 요구사항 (제3절)	1. 민감한 신용카드 정보	1.1	5.1.1 민감한 신용카드 기밀성	
		1.2	5.1.2 민감한 신용카드 정보 저장 금지	
		1.3	5.1.2 민감한 신용카드 정보 출력 금지	
	2. 신용카드 정보	2.1	5.4.1 신용카드 번호 암호화 등 전송 보호	
		2.2	5.4.2 신용카드 번호 암호화 등 저장	
		2.3	5.4.2 신용카드 번호 저장기간	
		2.4	5.4.3 신용카드 번호 삭제 및 파기	
		2.5	5.4.4 마스킹된 신용카드 번호 화면 표시	
			5.4.5 마스킹된 신용카드 번호 매출전표 출력	
	3. 암호화	3.1	5.2.1 112비트 이상의 보안강도	
		3.2	5.2.2 암호키 생성·분배	
		3.3	5.3.2 암호키 등 삭제 및 파기	
		3.4	5.3.1 암호키에 대한 비인가 접근 불가	
	4. 자체보호	4.1	5.5.1 무결성 점검	
		4.2	5.5.1 무결성 점검결과 제공	
		4.3	5.5.2 무결성 검증 실패 대응행동	
관리적 요구사항 (제4절)	1. 안전한 소프트웨어 개발	1.1	4.5 안전한 CAT/POS 단말기 개발	
	2. 초기 암호키 주입	2.1	4.5 안전한 CAT/POS 단말기 개발 및 운영	
		2.2	4.5 안전한 CAT/POS 단말기 개발 및 운영	
	3. 보안교육	3.1	4.5 보안교육	
	4. 형상관리	4.1	4.5 안전한 CAT/POS 단말기 개발 및 운영	
		4.2	4.5 안전한 CAT/POS 단말기 개발 및 운영	
		4.3	4.5 안전한 CAT/POS 단말기 개발 및 운영	
	5. 안전한 운영환경 구성	5.1	4.5 안전한 CAT/POS 단말기 운영	
		5.2	4.5 안전한 CAT/POS 단말기 운영	
		5.3	4.5 안전한 CAT/POS 단말기 운영	
		5.4	4.5 안전한 CAT 단말기 운영	N/A
	6. 보안취약점 점검 및 조치	6.1	4.5 안전한 CAT/POS 단말기 운영	
		6.2	4.5 안전한 CAT/POS 단말기 운영	

부록. 신용카드 단말기 유형별 보안기능 및 시험요구사항

부록1. CAT 단말기 보안기능 및 시험요구사항

1. 목적

본 문서는 신용카드 가맹점에서 신용카드 등의 거래승인을 위해 사용되는 결제용 CAT 단말기 제품의 운영환경요구사항, 필수 보안요구사항, 시험요구사항 및 권고사항을 정의한다. 이를 통해 신용카드 가맹점에서 취급되는 신용카드 등의 정보에 대하여 제3자에 의한 정보유출을 방지하고 신용카드 결제 시장의 안정화를 목적으로 한다.

- **카드사**는 가맹점 관리의무의 일환으로 가맹점으로 하여금 신용카드회원 등의 제3자 정보 유출에 대비한 보안대책을 수립하여야 하므로 본 보안기능 및 시험요구사항을 준수하고, 여신금융협회에 등록된 단말기에 의한 거래에 한하여 승인 하여야 한다.
- **CAT 단말기 공급업체**는 본 시험요구사항 및 보안표준을 준수하고 여신금융협회에 등록된 단말기를 가맹점에 유통 및 유지.보수하여야한다.
- **개발업체**는 본 문서에 기술된 CAT 단말기 제품의 운영환경 및 보안기능을 참조하여 제품을 구현하고, 여신금융협회의 시험・인증을 거쳐야 한다.
- **가맹점**은 단말기가 보안표준을 준수하고, 여신금융협회에 등록된 단말기인지 여부(스티커 등 표시)를 확인하여야 한다.

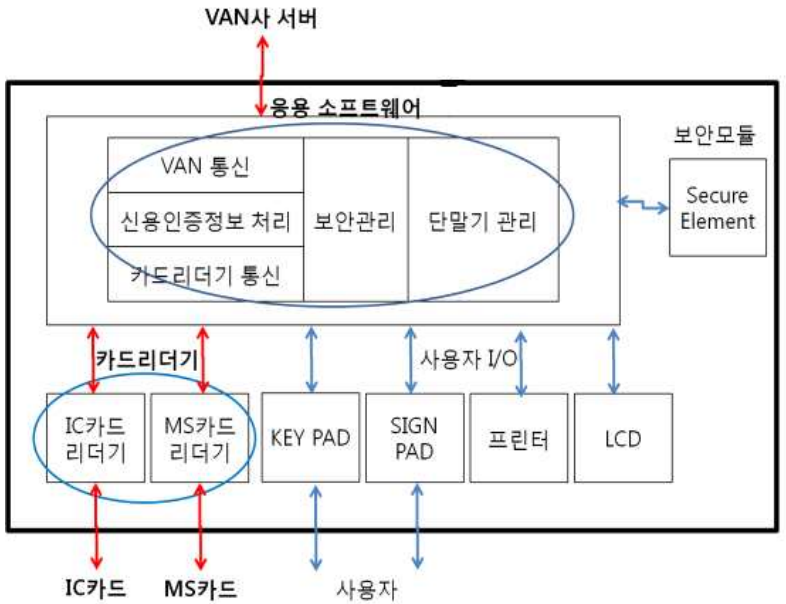
2. 적용범위

1. 본 보안기능 및 시험요구사항에서 칭하는 "CAT 단말기"는 단말기 본체 내부에 카드리더기를 내장한 CAT 단말기를 의미한다.
2. 본 보안기능 및 시험요구사항은 신용카드 가맹점에서 신용카드 거래승인을 위하여 결제용으로 사용하는 CAT 단말기에 적용한다. 단, CAT 단말기 중 보안기능수행과 관련 없는 부분은 시험범위에서 제외한다.
   (예시 : EMV Level1, Level2 인증서를 통해서 기 확인된 일부사항 등)
3. 본 시험요구사항에서 칭하는 "신용카드"는 신용카드, 체크카드, 선불카드(기프트카드)를 포함한다.

3. 제품개요

신용카드 결제기능과 관련된 CAT 단말기의 주요 보안 기능으로는 민감한 신용카드 정보 보호, 암호연산 및 암호키 생성/분배, 암호키 접근통제 및 파기, 신용카드 번호 보호, 자체보호 등이 있다.

아래 [그림 3]은 일반적인 CAT 단말기의 구조를 나타내고 있다. 본 문서에서 정의하고 있는 CAT 단말기 보안기능 요구사항의 적용범위는 1) 카드리더기로 부터 읽혀진 민감한 신용카드 정보가 응용소프트웨어로 전송되는 구간, 2) CAT 단말기 내에 위치한 CAT 단말기 응용소프트웨어에서 해당 정보가 처리되는 구간, 3) CAT 단말기와 VAN사 서버 간 민감한 신용카드 정보 전송 구간이다.



[그림 3] 일반적인 CAT 단말기 구조

4. CAT 단말기 운영환경 요구사항

4.1 신용카드 거래승인

4.1.1 CAT 단말기는 ISO7816에서 규정한 ID-1 TYPE 형태의 카드가 이용되는 경우 EMV 거래로 우선 처리하는 것을 원칙으로 한다. 그 외 형태의 카드가 이용되는 경우에도 CAT 단말기는 본 문서에서 요구하는 보안기능요구사항을 충족하여야 한다.

※ 응용 시 주의사항 : 비정상적 fall-back거래의 금지(정상적인 fall-back거래는 예외적으로 가능), 변칙적 M/S 거래의 금지

☞ **"IC우선거래 처리 방법"**

IC카드임에도 불구하고 MS카드로 거래가 시도되는 경우, MS카드 track2 data 중 서비스코드(2xx, 6xx)를 체크하여 IC카드로 거래할 수 있도록 유도한다.

※ IC카드와 통신하여 track2 equivalent data를 얻어온 후, 해당 정보를 바탕으로 MS거래로 변환 후 거래 시도 등은 허용하지 않는다.

☞ **"비정상적인 fall-back 거래"의 예**

정상적인 fall-back 거래로 인정될 수 없는 경우의 예는 다음과 같다.

① Chip 또는 Application이 block되어 있는 경우
② 카드자체가 block된 경우

☞ **"정상적인 fall-back 거래"의 예**

정상적인 fall-back 거래로 인정될 수 있는 경우의 예는 다음과 같다.

① Chip 전원을 넣었으나 응답이 없을 경우
② 상호지원 Application이 없을 경우
③ Chip 데이터 읽기 실패
④ Mandatory 데이터 미포함
⑤ CVM command 응답 실패
⑥ EMV command 잘못 설정
⑦ 터미널 오작동

4.2 신용카드 거래의 안전성 및 호환성 보장

4.2.1 CAT 단말기는 신용카드 거래의 안전성 및 호환성을 보장해야 한다.

☞ **CAT 단말기 "신용카드 거래의 안전성 및 호환성" 수준**

CAT 단말기가 국내에서 발급하는 접촉식 또는 비접촉식 신용카드를 지원하는 경우 EMV(L1/L2) 인증 또는 이에 준하는 방식으로 신용거래의 안전성 및 호환성을 보장해야 한다.

4.3 모든 종류의 신용카드 수용

4.3.1 CAT 단말기는 원칙적으로 국내에서 발급되는 모든 종류의 신용카드를 수용하여야 한다.

※ VISA, MASTER, JCB, GLOBAL, AMEX, 은련 등을 포함

※ 해외카드의 경우, 별도 기준을 준수하여야 한다.

4.4 선불카드 잔액표시

4.4.1 CAT 단말기는 선불카드(기프트 카드) 거래 시 잔액을 표시할 수 있어야 하며 회원용 매출표에 선불카드(기프트 카드) 잔액을 표시하여야 한다.

4.5 안전한 CAT 단말기 개발 및 운영, 보안 교육

4.5.1 CAT 단말기 개발업체는 안전한 CAT 단말기 프로그램 개발을 위해 개발단계부터 취약점의 원인을 배제하도록 소프트웨어 개발보안 방법론을 채택하여 개발해야 한다. 또한, CAT 단말기 운영환경을 안전하게 구성하는 방법과 관리자 보안 인식제고 및 내부자 교육 계획을 수립해야 한다.

4.5.2 개발업체는 원칙적으로 해당 사항에 대한 계획을 수립하여 이행할 것을 권고한다.

☞ **소프트웨어 개발보안 관련 주요 참고자료**

① (국내) 소프트웨어 개발보안 가이드 및 시큐어코딩 가이드(행정안전부·한국인터넷진흥원)

② (국외) C/C++/JAVA Secure Coding Guide, CERT(카네기멜론대학교 SEI연구소)

③ (국외) Secure Coding Guide, OWASP

5. CAT 단말기 보안기능 시험요구사항

5.1. 민감한 신용카드 정보 보호

민감한 신용카드 정보의 안전성을 보장하기 위해 다음의 요구사항을 만족해야 한다.

5.1.1 민감한 신용카드 정보의 기밀성은 민감한 신용카드 정보 전송구간 전체에서 유지되어야 한다.

※ 응용 시 주의사항: 민감한 신용카드 정보 전송구간은 1) 민감한 신용카드 정보가 CAT 단말기에 내장된 카드리더기를 통하여 읽혀진 시점부터 CAT 단말기 내부에서 처리되는 구간,

☞ **"민감한 신용카드 정보" 전송구간(CAT 단말기 내장 카드리더기→CAT 단말기 내부)의 기밀성 보증 수준**

민감한 신용카드 정보가 CAT 단말기에 내장된 카드리더기를 통하여 읽혀지는 시점부터 CAT 단말기 내부에서 처리되는 구간 내에서 기밀성 보증 수준은 다음과 같다.

① MS카드 또는 IC카드로부터 CAT 단말기에 내장된 MS카드리더기 또는 IC카드리더기를 통하여 민감한 신용카드 정보를 입력 받은 CAT단말기는 해당 정보를 112비트 이상의 보안강도 암호알고리즘을 이용하여 CAT단말기 내부에서 암호화 하여야 한다.

② 112비트 이상의 보안강도를 갖는 암호알고리즘으로 암호화 된 민감한 신용카드 정보는 CAT 단말기 내부에서 복호화 될 수 없다.

③ CAT단말기는 CAT단말기 외부 인터페이스(USB Port, JTAG Port 등)를 통한 CAT 단말기 내부에 대한 비인가된 논리적 접근 시도를 방어해야 한다.

2) CAT 단말기로부터 VAN사 서버로 전송되는 구간을 의미하며 기밀성이 유지된 민감한 신용카드 정보는 전송구간 전체에서 복호화 될 수 없으며 평문으로 존재하는 구간이 없어야 한다.

☞ **"민감한 신용카드 정보" 전송구간(CAT 단말기→VAN사 서버)의 기밀성 보증 수준**

CAT 단말기로부터 VAN사 서버로 전송되는 구간의 기밀성 보증 수준은 다음과 같다.

① 112비트 이상의 보안강도로 암호화된 민감한 신용카드 정보는 CAT 단말기와 통신하는 VAN사 서버에서만 신용카드 거래 요청의 목적으로 복호화 될 수 있다.

② 통신 중개 등을 목적으로 CAT 단말기 본체로부터 VAN사 서버까지의 민감한 신용카드 정보 전송구간 상에 존재하는 어떠한 서버(예-EDI 가맹점 중계서버)도 암호화된 민감한 신용카드 정보를 복호화 할 수 없다.

5.1.2 CAT 단말기는 민감한 신용카드 정보를 저장하거나 출력하지 않아야 한다.

※ 응용 시 주의사항 : 1. CAT 단말기는 신용거래 승인 시 출력하는 모든 전표에 민감한 신용카드 정보를 출력하지 않아야 한다. 2. CAT 단말기는 신용카드 거래 승인시점부터 민감한 신용카드 정보를 저장하지 않아야 하며 메모리에서 삭제해야 한다.

☞ **민감한 신용카드 정보의 저장 및 출력 금지**

① 민감한 신용카드 정보는 CAT단말기 내부에서 파일형태로 저장될 수 없으며 암호화 된 경우에도 파일형태로 저장될 수 없다.

② 민감한 신용카드 정보는 신용카드 거래 승인시점 이후 카드리더기 내부 메모리에서 완전 삭제되어야 하며 암호화된 경우에도 카드리더기 내부 메모리에서 완전 삭제되어야 한다.

☞ 민감한 신용카드 정보의 저장 및 출력 금지

③ 암호화된 민감한 신용카드 정보는 CAT 단말기 본체에 파일형태로 저장될 수 없다. 단, 민감한 신용카드 정보 중 신용카드 번호는 마스킹 되어 CAT 단말기 본체 내부에 파일 형태로 저장될 수도 있다. (5.4 신용카드 번호 보호 참고)

④ 민감한 신용카드 정보는 신용거래 승인 시 출력하는 모든 전표에 출력될 수 없으며 암호화 된 경우에도 모든 전표에 출력될 수 없다. 단, 민감한 신용카드 정보 중 신용카드 번호는 마스킹 되어 전표에 출력될 수 있다. (5.4 신용카드 번호 보호 참고)

☆♣ "민감한 신용카드 정보 보호" 시험요구사항

개발업체는 개발한 CAT 단말기가 "민감한 신용카드 정보 보호" 보안요구사항을 만족하고 있음을 증명하여야 한다. 개발업체는 암호화 대상 정보, 적용 암호알고리즘 및 CAT 단말기에서 VAN사까지의 암호화 방식 등을 기술한 문서를 시험기관에 제공하여야 한다. 개발업체는 해당 기능에 대한 시험 증거자료 및 추가적으로 시험기관에서 정의한 시험지원 자료를 시험기관에 제공하여야 한다.

5.2 암호 연산 및 암호키 생성/분배

민감한 신용카드 정보의 기밀성을 제공하기 위하여 사용되는 암호연산 및 암호키는 다음의 요구사항을 만족해야 한다.

5.2.1 민감한 신용카드 정보는 112비트 이상의 보안강도를 갖는 암호알고리즘과 암호키 길이에 따라 암호화 되어야 한다.

※ 응용 시 주의사항 : 민감한 신용카드 정보에 대한 암호화 시 동일한 암호문이 생성되지 않아야 한다.

☞ "112비트 이상의 보안강도를 갖는 암호알고리즘"

112비트 이상의 보안강도를 갖는 암호알고리즘 목록은 암호모듈검증 대상 보호함수 (국가사이버안전센터)와 최신버전의 '암호 알고리즘 및 키길이 이용안내서(한국인터넷진흥원)'를 참고한다.

① 암호알고리즘의 보안강도란 암호 알고리즘이나 시스템의 암호키 또는 해쉬함수의 취약성을 찾아내는데 소요되는 작업량을 수치화한 것을 의미하며 112비트의 보안강도란 2^{112}번의 계산 수행을 통하여 암호키 또는 암호 알고리즘의 취약성을 알아낼 수 있음을 의미한다.

② 국내에서 권고하는 112비트 이상의 보안강도를 갖는 암호알고리즘의 목록은 다음과 같다.

1. 대칭키 암호알고리즘은 AES-128/192/256, 3TDEA, SEED, HIGHT, ARIA-128/192/256이다.
2. 암/복호화를 위한 공개키 알고리즘은 RSAES-OAEP 2048이다.
   - o RSAES-OAEP에서 사용하는 해쉬함수는 SHA-224/256/384/512이다.
   - o HAS-160, SHA-1도 112비트에 포함되나 충돌 저항성이 112비트 보안강도를 제공하지 못하므로 사용하지 않는 것을 권장한다.
3. ECC 알고리즘은 전자서명용으로만 권고하고 있음으로, 민감한 신용카드 정보 암/복호화를 위한 공개키 알고리즘으로는 사용하지 않는 것을 권고한다.

5.2.2 안전성이 검증된 암호키 생성/분배 방법이 사용되어야 한다.

☞ "안전성이 검증된 암호키 생성/분배 방법"

안전성이 검증된 암호키 생성/분배 방법이라 함은 다음과 같다.

① 국내외 표준 또는 가이드문서 또는 보안표준에 준하는 문서 등에서 권고하고 있는 암호키 생성/분배 방법

※ 암호 알고리즘 및 키 길이 이용 안내서(한국인터넷진흥원, 2013.6.28)"에서는 공개키 기반의 키 공유 알고리즘인 DH 및 ECDH를 권고하고 있다.

※ 관련된 국외 표준 등은 ISO/IEC 11770-3(2008), PKCS#1, PKCS#3 등이 있다.

② 국내 암호모듈검증 제도에 따라 검증받은 암호키 생성/분배 방법

※ KSX ISO/IEC 19790 : 2007, 정보기술-보안기술-암호모듈보안 요구사항

③ 기타 국내외 전문기관에서 안전성을 검증 받은 암호키 생성/분배 방법

☞ "암호키 수명(생명주기)"

민감한 신용카드 정보 암호화에 사용되는 암호키는 적절한 암호키 수명(생명주기)을 가져야 한다. 적절한 암호키 수명이란 국내외 전문기관에서 권고하고 있는 암호키의 유효기간을 의미한다.

※ NIST SP 800-57(Recommendation for Key Management: Part 1 : General (Revision3), 2012.7), KISA 암호이용 안내서(2013.12) 등에서는 암호키 수명에 대한 권고사항을 기술하고 있다.

☆♣ "암호 연산 및 암호키 생성/분배" 시험요구사항

개발업체는 개발한 CAT 단말기가 "암호 연산 및 암호키 생성/분배" 보안요구사항을 만족하고 있음을 증명하여야 한다. 개발업체는 사용 암호알고리즘의 보안강도, 암호키 생성/분배 방법의 안전성 근거 자료 등을 기술한 문서를 시험기관에 제공하여야 한다. 개발업체는 사용하는 암호알고리즘의 구현 적합성 관련 시험 증거자료 및 추가적으로 시험기관에서 정의한 시험지원 자료를 시험기관에 제공하여야 한다.

5.3 암호키 접근 통제 및 파기

민감한 신용카드 정보 암호키의 안전성을 보장하기 위해 다음의 요구사항을 만족해야 한다.

5.3.1 암호키에 대한 인가되지 않은 접근은 허용되지 않아야 한다.

※ 응용 시 주의사항:

1. 암호키에 대한 물리적/논리적 접근은 인가된 관리자/프로그램 등에게만 허용되어야 한다.
2. 민감한 신용카드 정보 암호화를 목적으로 사용되는 암호키는 안전하게 저장/관리되어야 하며, CAT 단말기는 암호키에 대한 비인가 된 접근시도를 방어해야 한다.

☞ "비인가된 암호키 접근시도에 대한 방어"

① CAT단말기 내부에 저장되는 암호키는 암호화되어 저장되어야 한다.

② CAT단말기는 CAT단말기 외부 인터페이스(USB Port, JTAG Port 등)를 통한 CAT단말기 내부에 대한 비인가된 논리적 접근 시도를 방어해야 한다.

3. 안전성이 검증된 암호키 접근통제 방법이 사용되어야 한다.

☞ **"안전성이 검증된 암호키 접근통제 방법"**

안전성이 검증된 암호키 접근통제 방법은 다음과 같다.

① 암호키 접근통제를 위한 스마트카드, 보안토큰과 같은 템퍼 프루프(Tamper-Proof) 매체의 사용
② 국내외 표준 또는 가이드문서 또는 보안표준에 준하는 문서 등에서 권고하고 있는 암호키에 대한 접근통제 방법
③ 기타 국내외 전문기관에서 안전성을 검증 받은 암호키 접근통제 방법

5.3.2 사용이 만료/종료된 암호키 및 암호키 생성/분배를 위해 사용된 모든 정보는 CAT 단말기에서 삭제(파기)되어야 한다.

☞ **"암호키 생성/분배에 사용된 정보"의 삭제**

암호키 생성/분배를 위해 사용된 모든 정보란 키 길이, 키 종류, 유효기간 등을 의미하며 CAT 단말기에서 암호키 생성/분배를 위해 사용된 모든 정보는 사용 만료/종료된 후 삭제(파기)되어야 한다.

※ 응용 시 주의사항: 1. 안전성이 검증된 암호키 삭제 방법이 사용되어야 한다.

☞ **"안전성이 검증된 암호키 삭제 방법"**

안전성이 검증된 암호키 삭제 방법 중 대표적인 예는 키를 '0' 등의 특정 문자로 채운 후 해당 메모리를 해제하는 방법이다.

☆♣ **"암호키 접근통제 및 파기" 시험요구사항**

개발업체는 개발한 CAT 단말기가 "암호키 접근통제 및 파기" 보안요구사항을 만족하고 있음을 증명하여야 한다. 개발업체는 사용하는 암호키 접근통제 및 파기 방법, 사용 방법의 안전성 근거 자료 등을 기술한 문서를 시험기관에 제공하여야 한다. 개발업체는 관련 시험 증거자료 및 추가적으로 시험기관에서 정의한 시험지원 자료를 시험기관에 제공하여야 한다.

5.4 신용카드 번호 보호

신용카드 번호를 보호하기 위하여 다음의 요구사항을 만족해야 한다.

5.4.1 신용카드 번호는 신용카드 번호 전송구간 전체에서 암호화, 마스킹, 전용망을 이용한 전송 등의 방법으로 보호되어 전송되어야 한다.

☞ **"신용카드 번호"의 보호**

① 보안요구사항 5.1.1에 따라 신용카드 번호는 민감한 신용카드 정보로 포함되어 암호화 되고 전송보호 되어야 한다.
② '신용카드 번호'가 카드사가 승인한 매입 업무 처리, 카드사 제휴서비스 연계, 전표 출력의

☞ **"신용카드 번호"의 보호**

목적으로 POS 단말기 본체/POS 서버 등으로 전송이 필요한 경우,
'신용카드 번호' 전체 또는 일부는 민감한 신용카드 정보와 별도로 카드리더기로부터 읽혀진 후, POS 단말기 본체/POS 서버 등으로 전송될 수 있다.
단, 추가적으로 전송되는 '신용카드 번호'는 암호화, 마스킹, 전용망을 이용한 전송 등의 방법으로 보호되어 전송구간 내에서 전송되어야 한다.

※ 응용 시 주의사항: 신용카드 번호 전송구간은 신용카드 번호가 카드리더기를 통하여 읽혀지는 시점부터 VAN사 서버로 전송되는 구간 전체를 의미한다. 각 전송구간별 신용카드 번호의 전송 보호 수준은 시험요구사항을 참조한다.

☞ **"신용카드 번호" 전송구간(카드리더기→VAN사 서버)의 전송 보호 수준**

추가적으로 전송되는 '신용카드 번호'에 대한 전송 보호 수준은 다음과 같다.

① 신용카드 번호가 암호화 되지 않는 무선망, 일반 인터넷 망 등 OPEN망/구간을 통하여 전송구간 내에서 전송되는 경우, '신용카드 번호' 전부는 암호화되거나 일부 마스킹되어 전송되어야 한다.
※ 'OPEN 망/구간'의 예는 다음과 같다.
1. 일반 인터넷 망으로 연결된 가맹점과 VAN사 또는 가맹점과 카드사 구간
2. 일반 인터넷 망으로 연결된 CAT 단말기와 POS서버 구간
※ '신용카드 번호' 암호화 시, '신용카드 번호'는 카드사가 승인한 매입 업무, 카드사 제휴서비스 연계 처리 등의 목적으로 사용하는 주체의 키로 암호화될 수 있으며 112비트 이상의 보안강도를 갖는 암호알고리즘과 암호키 길이에 따라 암호화 되어야 한다. (보안요구사항 5.2 참조)
※ '신용카드 번호' 마스킹 시, 신용카드 번호 전체 자리 중 7번째에서 12번째 번호는 '*'로 마스킹 되어야 한다.
② 신용카드 번호가 전송구간 내에서 전용망 (또는 전용망으로 간주될 수 있는 전송선로)을 이용하여 전송되는 경우, 신용카드 번호는 암호화 되지 않거나 마스킹 되지 않고 전송될 수 있다.
※ '전용망(또는 전용망으로 간주될 수 있는 전송선로)'의 예는 다음과 같다.
1. CAT 단말기와 VAN사간 전화선 연결구간
2. VPN 암호화 통신 구간
3. 전용망으로 연결된 CAT 단말기와 POS서버 또는 CAT 단말기와 VAN사 또는 CAT 단말기와 카드사 구간
4. 전용망으로 연결된 POS서버와 VAN사 또는 POS서버와 카드사 구간

☞ **"카드사 제휴서비스 처리 방법의 예"**

① CAT 단말기는 신용카드 거래를 위해 읽어온 track2 (equivalent) data 중 신용카드번호/제휴(상품)코드/OCB(OK CashBag) 구분자 등을 전송구간 내 존재하는 별도 단말기에 "신용카드 번호" 전송 보호 수준에 따라 전송한다.
② 해당 정보를 전송받은 단말기는 전송된 카드 BIN 또는 제휴(상품)코드 등을 확인하여 선할인, 포인트 적립 등 제휴서비스 업무를 처리한다.

5.4.2 신용카드 번호는 신용카드 번호 전송구간 전체에서 암호화, 마스킹, 거래를 구분할 수 있는 다른 정보로 변환 등의 방법으로 보호되어 저장되어야 한다.

☞ **"신용카드 번호"의 보호**

① 보안요구사항 5.1.1에 따라 민감한 신용카드 정보로 포함되어 암호화 된 신용카드 번호는 보안요구사항 5.1.2에 따라 신용카드 번호 전송구간 전체에서 어떠한 형태로도 저장될 수 없다.

② '신용카드 번호'가 카드사가 승인한 매입 업무 처리, 카드사 제휴서비스 연계의 목적으로 POS 서버 등에 저장이 필요한 경우,
'신용카드 번호' 전체 또는 일부는 민감한 신용카드 정보와 별도로 카드리더기로 부터 읽혀진 후, POS 서버 등으로 전송된 후 저장될 수 있다.
단, 추가적으로 전송된 후 저장되는 '신용카드 번호'는 암호화, 마스킹, 거래를 구분할 수 있는 다른 정보로 변환 등의 방법으로 보호되어 저장되어야 한다.

※ 응용 시 주의사항: 1. 신용카드 번호 전송구간 내에서의 신용카드 번호 저장은 업무상 필요성이 인정되는 경우에만 허용된다. 각 전송구간별 신용카드 번호의 저장 보호 수준은 시험요구사항을 참조한다.

☞ **"신용카드 번호" 전송구간(카드리더기→VAN사 서버)의 저장 보호 수준**

추가적으로 전송된 후 저장되는 '신용카드 번호'에 대한 저장 보호 수준은 다음과 같다.

① 신용카드 번호가 전송구간 내에서 암호화 되지 않는 무선망, 일반 인터넷 망 등 OPEN망/구간을 이용하여 전송되는 경우, '신용카드 번호'는 일부 마스킹되거나, 거래를 구분할 수 있는 다른 정보로 변환되어 저장되어야 한다.
※ 'OPEN 망/구간'의 예는 보안요구사항 5.4.1과 같다.
※ '신용카드 번호' 마스킹 저장 시, 신용카드 번호 전체 자리 중 7번째에서 12번째 번호는 '*'로 마스킹되어 저장되어야 한다.
※ 거래를 구분할 수 있는 다른 정보로 변환되어 저장되는 예
1. 신용카드 번호에 대한 해쉬(HASH)값. 단, 충돌 저항성이 112비트 보안강도 이상인 해쉬 알고리즘 사용 권고
2. VAN사 또는 카드사에서 거래 구분 시 사용하는 값
3. 기타 거래를 구분할 수 있는 다른 정보로 인정될 수 있는 값

② 신용카드 번호가 전송구간 내에서 전용망 (또는 전용망으로 간주될 수 있는 전송선로)을 이용하여 전송되는 경우, 신용카드 번호는 암호화 되거나, 일부 마스킹되어 저장되어야 한다.
※ '전용망(또는 전용망으로 간주될 수 있는 전송선로)'의 예는 보안요구사항 5.4.1과 같다.
※ '신용카드 번호' 암호화 저장 시, '신용카드 번호'는 카드사가 승인한 매입 업무 처리, 카드사 제휴서비스 연계의 목적으로 사용하는 주체(예-가맹점)의 키로 암호화될 수 있으며 112비트 이상의 보안강도를 갖는 암호알고리즘과 암호키 길이에 따라 암호화 되어 저장되어야 한다. (보안요구사항 5.2 참조)
※ '신용카드 번호' 마스킹 저장 시, 신용카드 번호 전체 중 7번째에서 12번째 번호는 '*'로 마스킹되어 저장되어야 한다.

2. 저장이 허용되는 경우, 신용카드 번호는 암호화, 마스킹, 거래를 구분할 수 있는 다른 정보로 변환 등으로 보호되어 일정기간만 저장되어야 한다.

☞ **"신용카드 번호" 저장 기간**

신용카드 번호 전송구간 내에서 '신용카드 번호'가 암호화, 마스킹, 거래를 구분할 수 있는 다른 정보로 변환되어 저장할 수 있는 기간은 최대 3개월이다.

3. 저장 기간이 만료된 경우, 해당정보는 저장소에서 완전 삭제되어야 한다.

☞ **"암호화 또는 마스킹 등으로 보호된 신용카드 번호의 완전삭제"**

완전삭제의 의미는 다음과 같다.

① 완전삭제란 저장 공간(파일시스템)에 저장된 해당 정보의 기록영역을 0 또는 랜덤한 값으로 덮어쓰는 방법을 의미한다.

② 대표적인 완전삭제 방법은 DoD 5220.22-M(또는 DoD 5200.28-STD)이며, 본 요구사항에서는 최소 3회 이상의 덮어쓰기를 권고한다.

5.4.3 CAT 단말기는 승인 완료된 거래에 대해 거래 종료 시점에 신용카드 번호가 더 이상 가용되지 않도록 메모리에서 삭제(파기)해야 한다.

☞ **"승인 완료된 거래의 신용카드 정보 파기"**

승인 완료된 거래란 POS 단말기로부터 요청된 신용거래가 완료되어 CAT 단말기 모니터 화면의 표시 및 매출전표의 출력이 이루어진 거래를 의미한다.
CAT단말기는 승인 완료 후 신용카드 번호를 메모리에서 파기해야한다.

5.4.4 신용카드 번호를 CAT 단말기 모니터 화면에 표시하는 경우 신용카드 번호는 아래 "응용 시 주의사항"에 명시된 방식으로 마스킹 되어야 한다.

※ 응용 시 주의 사항: 신용카드 카드번호 전체 자리 중 7번째에서 12번째 번호는 '*'로 마스킹되어야 한다.

5.4.5 매출 전표 출력 시 신용카드 번호는 아래 "응용 시 주의사항"에 명시된 방식으로 마스킹되어 출력하여야 한다.

※ 응용 시 주의 사항: 신용카드 카드번호 전체 자리 중 7번째에서 12번째 번호는 '*'로 마스킹되어야 한다.

☆♣ **"신용카드 번호 보호" 시험요구사항**

개발업체는 개발한 CAT 단말기가 "신용카드 번호 보호" 보안요구사항을 만족하고 있음을 증명하여야 한다. 개발업체는 마스킹된 신용카드 번호 보호 체계, 삭제 주기, 삭제 방법 메커니즘 등을 기술한 문서를 시험기관에 제공하여야 한다. 개발업체는 관련 시험 증거자료 및 추가적으로 시험기관에서 정의한 시험지원 자료를 시험기관에 제공하여야 한다.

5.5 자체보호

CAT 단말기의 정상적인 동작을 보장하기 위하여 다음의 요구사항을 만족해야 한다.

5.5.1 CAT 단말기는 시동 시 및 [선택 : 주기적으로, 관리자 요청 시] 보안기능 실행코드 및 보안기능 관련 저장데이터(보안기능 관련 프로그램 설정값 등) 변경 여부를 탐지하기 위한 무결성 점검을 수행하여야 하며 수행결과를 관리자가 조회할 수 있어야한다.

☞ "CAT 단말기의 무결성 점검"

CAT 단말기의 무결성 점검이란 보안기능을 수행하는 CAT 단말기의 보안기능 실행코드, 보안기능 관련 설정 값 등의 무단 생성 및 변경, 삭제 여부를 점검함을 의미한다.

① 보안기능 관련 저장데이터는 알람 규칙, 정책 설정 등이 있으며 보안기능 관련 저장데이터는 파일시스템에 평문으로 존재할 수 없다.

② 무결성 점검을 주기적으로 수행할 시 간격은 기본적으로 설정된 시간 마다 (예 : 6시간 마다) 혹은 인가된 관리자에 의해 설정된 시간(예: 매일 특정시간)마다 수행한다.

5.5.2 CAT 단말기는 무결성 검증 실패 시 동작 중단 및 CAT 단말기 관리자에게 해당내용을 자동으로 통보해야한다.

☞ "CAT 단말기의 무결성 검증 실패 시 대응 방안"

무결성 점검 결과 변조탐지 및 무결성 검증 동작 실패 시 CAT 단말기 동작 중단과 함께 결과를 관리자에게 경고음 또는 화면 출력 등으로 통보해야 한다.

☆♣ "자체보호" 시험요구사항

개발업체는 개발한 CAT 단말기가 "자체보호" 보안요구사항을 만족하고 있음을 증명하여야 한다. 개발업체는 무결성 보호 대상 목록, 무결성 검사 메커니즘 등을 기술한 문서를 시험기관에 제공하여야 한다. 개발업체는 관련 시험 증거자료 및 추가적으로 시험기관에서 정의한 시험지원 자료를 시험기관에 제공하여야 한다.

부록2. POS 단말기 보안기능 및 시험요구사항

1. 목적

본 문서는 신용카드 가맹점에서 신용카드 거래승인을 위해 사용되는 결제용 POS 단말기 제품의 운영환경요구사항, 필수 보안요구사항, 시험요구사항 및 권고사항을 정의한다. 이를 통해 신용카드 가맹점에서 취급되는 신용카드 등의 정보에 대하여 제3자에 의한 정보유출을 방지하고 신용카드 결제 시장의 안정화를 목적으로 한다.

- **카드사**는 가맹점 관리의무의 일환으로 가맹점으로 하여금 신용카드회원 등의 제3자 정보유출에 대비한 보안대책을 수립하여야 하므로 본 보안기능 및 시험요구사항을 준수하고, 여신금융협회에 등록된 단말기에 의한 거래에 한하여 승인 하여야 한다.
- **POS 단말기 공급업체는** 본 보안요구사항 및 시험요구사항을 준수하고 여신금융협회에 등록된 단말기를 가맹점에 유통 및 유지.보수하여야한다.
- **개발업체**는 본 문서에 기술된 POS 단말기 제품의 운영환경 및 보안기능을 참조하여 제품을 구현하고, 여신금융협회의 시험・인증을 거쳐야 한다.
- **가맹점**은 단말기가 보안표준을 준수하고, 여신금융협회에 등록된 단말기인지 여부(스티커 등 표시)를 확인하여야 한다.

2. 적용범위

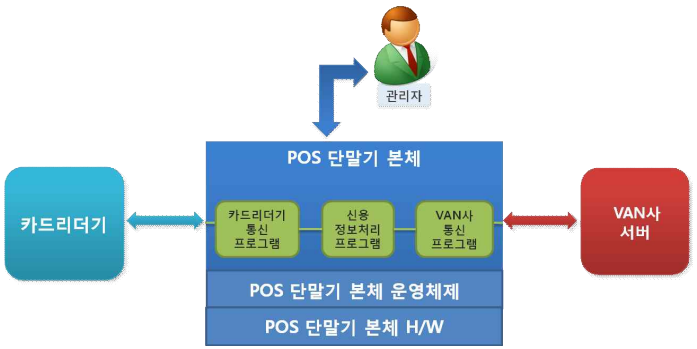
1. 본 보안기능 및 시험요구사항에서 칭하는 "POS 단말기"는 POS 단말기 본체와 카드리더기를 포함한다.
2. 본 보안기능 및 시험요구사항은 POS 단말기 중 신용카드 가맹점에서 신용카드 거래승인을 위하여 결제용으로 사용하는 POS 단말기에 적용한다. POS 단말기 중 신용카드 결제전송 기능이 설치되지 않았거나, 신용카드 거래승인과 관련이 없는 POS 단말기는 적용대상에서 제외된다.
3. 본 보안기능 및 시험요구사항에서 정의하는 시험범위는 카드리더기와 POS 단말기 본체에 설치된 카드리더기 통신 소프트웨어, VAN 통신 소프트웨어 등 POS 단말기 소프트웨어이다. 단, 카드리더기와 POS 단말기 소프트웨어 중 보안기능수행과 관련 없는 부분은 시험범위에서 제외한다. (예시 : EMV Level1, Level2 인증서를 통해서 기 확인된 일부사항 등)
4. 본 보안기능 및 시험요구사항에서 칭하는 "신용카드"는 신용카드, 체크카드, 선불카드(기프트카드)를 포함한다.

3. 제품개요

POS 단말기 제품(이하 POS 단말기)은 가맹점에 설치되어 판매상품조회, 매출조회 등 다양한 판매시점 관리기능과 신용카드에 의한 거래발생 건에 대하여 카드사로부터 거래승인을 받기 위하여 거래승인기능을 제공하는 단말 장치이다. POS 단말기는 신용카드 결제, 현금결제, 상품권 결제 등 다양한 금융결제기능과 관련된 금융정보를 취급하고 있으나 본 문서에서는 결제용 POS 단말기의 신용카드 결제 기능과 관련된 보안요구사항을 정의한다.

신용카드 결제기능과 관련된 POS 단말기의 주요 보안 기능으로는 민감한 신용카드 정보 보호, 암호연산 및 암호키 생성/분배, 암호키 접근통제 및 파기, 신용카드 번호 보호, 자체보호 등이 있다.

아래 [그림 4]은 POS 단말기의 운영환경을 나타내고 있다. POS 단말기는 물리적으로 일반 PC 또는 POS 전용 단말기 하드웨어 등의 POS 단말기 본체와 카드리더기로 구성되며 POS 단말기 본체와 카드리더기는 유·무선으로 연결되거나 카드리더기가 POS 단말기 본체에 내장될 수 있다. 본 문서에서 정의하고 있는 POS 단말기 보안기능 요구사항의 적용범위는 1) POS 단말기 본체에 연결된 카드리더기, 2) 카드리더기와 POS 단말기 본체 간 민감한 신용카드 정보 전송 구간, 3) POS 단말기 본체 내에 위치한 민감한 신용정보처리 소프트웨어, 카드리더기 및 VAN사 서버 통신 소프트웨어, 4) POS 단말기 본체와 VAN사 서버 간 민감한 신용카드 정보 전송 구간이다.



[그림 4] POS 단말기 운영환경

4. POS 단말기 운영환경 요구사항

4.1 신용카드 거래승인

4.1.1 POS 단말기는 ISO7816에서 규정한 ID-1 TYPE 형태의 카드가 이용되는 경우 EMV 거래로 우선 처리하는 것을 원칙으로 한다. 그 외 형태의 카드가 이용되는 경우에도 POS 단말기는 본 문서에서 요구하는 보안기능요구사항을 충족하여야 한다.

※ 응용시 주의사항 : 비정상적 fall-back거래의 금지(정상적인 fall-back거래는 예외적으로 가능), 변칙적 M/S 거래의 금지

☞ "IC우선거래 처리 방법"

IC카드임에도 불구하고 MS카드로 거래가 시도되는 경우, MS카드 track2 data 중 서비스코드(2xx, 6xx)를 체크하여 IC카드로 거래할 수 있도록 유도한다.

※ IC카드와 통신하여 track2 equivalent data를 얻어온 후, 해당 정보를 바탕으로 MS거래로 변환 후 거래 시도 등은 허용하지 않는다.

☞ "비정상적인 fall-back 거래"의 예

정상적인 fall-back 거래로 인정될 수 없는 경우의 예는 다음과 같다.

① Chip 또는 Application이 block되어 있는 경우
② 카드자체가 block된 경우

☞ "정상적인 fall-back 거래"의 예

정상적인 fall-back 거래로 인정될 수 있는 경우의 예는 다음과 같다.

① Chip 전원을 넣었으나 응답이 없을 경우
② 상호지원 Application이 없을 경우
③ Chip 데이터 읽기 실패
④ Mandatory 데이터 미포함
⑤ CVM command 응답 실패
⑥ EMV command 잘못 설정
⑦ 터미널 오작동

4.2 신용카드 거래의 안전성 및 호환성 보장

4.2.1 신용카드 거래승인 시 POS 단말기 본체와 유·무선에 의하여 연결된 카드리더기를 이용할 수 있으며, 이 경우 해당 카드리더기는 신용카드 거래의 안전성 및 호환성을 보장해야 한다.

☞ POS 단말기 "신용카드 거래의 안전성 및 호환성" 수준

카드리더기가 국내에서 발급하는 접촉식 또는 비접촉식 신용카드를 지원하는 경우 EMV(L1/L2) 인증 또는 이에 준하는 방식으로 신용거래의 안전성 및 호환성을 보장해야 한다.

4.3 모든 종류의 신용카드 수용

4.3.1 POS 단말기는 원칙적으로 국내에서 발급되는 모든 종류의 신용카드를 수용하여야 한다.

※ VISA, MASTER, JCB, GLOBAL, AMEX, 은련 등을 포함

※ 해외카드의 경우, 별도 기준을 준수하여야 한다.

4.4 선불카드 잔액표시

4.4.1 POS 단말기는 선불카드(기프트 카드) 거래 시 잔액을 표시할 수 있어야 하며 회원용 매출표에 선불카드(기프트 카드) 잔액을 표시하여야 한다.

4.5 안전한 POS 단말기 개발 및 운영, 보안 교육

4.5.1 POS 단말기 개발업체는 안전한 POS 단말기 프로그램 개발을 위해 개발단계부터 취약점의 원인을 배제하도록 소프트웨어 개발보안 방법론을 채택하여 개발해야 한다. 또한, POS 단말기 운영환경을 안전하게 구성하는 방법과 관리자 보안 인식제고 및 내부자 교육 계획을 수립해야 한다.

4.5.2 개발업체는 원칙적으로 해당 사항에 대한 계획을 수립하여 이행할 것을 권고한다.

☞ 소프트웨어 개발보안 관련 주요 참고자료

① (국내) 소프트웨어 개발보안 가이드 및 시큐어코딩 가이드(행정안전부·한국인터넷진흥원)

② (국외) C/C++/JAVA Secure Coding Guide, CERT(카네기멜론대학교 SEI연구소)

③ (국외) Secure Coding Guide, OWASP

5. POS 단말기 보안기능 시험요구사항

5.1. 민감한 신용카드 정보 보호

민감한 신용카드 정보의 안전성을 보장하기 위해 다음의 요구사항을 만족해야 한다.

5.1.1 민감한 신용카드 정보의 기밀성은 민감한 신용카드 정보 전송구간 전체에서 유지되어야 한다.

※ 응용 시 주의사항: 민감한 신용카드 정보 전송구간은 1) 민감한 신용카드 정보가 카드리더기를 통하여 읽혀지는 시점부터 POS 단말기 본체로 입력되는 구간

☞ "민감한 신용카드 정보" 전송구간(카드리더기→POS 단말기 본체)의 기밀성 보증 수준

민감한 신용카드 정보가 카드리더기를 통하여 읽혀지는 시점부터 POS 단말기 본체로 전송되는 구간의 기밀성 보증 수준은 다음과 같다.

① MS카드 또는 IC카드로부터 MS카드리더기 또는 IC카드리더기를 통하여 민감한 신용카드 정보를 입력 받은 카드리더기는 해당 정보를 112비트 이상의 보안강도 암호알고리즘을 이용하여 카드리더기 내부에서 암호화 하여야 한다.

② 카드리더기 외부 인터페이스를 통하여 민감한 신용카드 정보가 POS 단말기 본체로 입력되는 구간 내에서 해당 정보의 기밀성은 유지되어야 한다.

③ 카드리더기는 카드리더기 외부 인터페이스(USB Port, JTAG Port 등)를 통한 카드리더기 내부에 대한 비인가된 논리적 접근 시도를 방어해야 한다.

2) POS 단말기 본체 내에서 해당 정보가 처리되는 구간,

☞ "민감한 신용카드 정보" 전송구간(POS 단말기 본체)의 기밀성 보증 수준

POS 단말기 본체 내부 구간의 기밀성 보증 수준은 다음과 같다.

① POS 단말기 본체 내부 구간이라 함은 카드리더기 드라이버 및 통신 라이브러리, VAN사 통신 라이브러리, 해당 라이브러리 등을 이용하여 신용카드 전문 전송처리 기능 등을 수행하는 POS 프로그램이 설치되어 동작하는 POS 단말기 본체 내부를 의미한다.

② POS 단말기 본체에 설치된 어떠한 소프트웨어(POS 프로그램 등) 및 하드웨어 장치도 112비트 이상의 보안강도로 암호화된 민감한 신용카드 정보를 복호화 할 수 없다.

3) POS 단말기 본체로부터 VAN사 서버로 전송되는 구간을 의미하며 기밀성이 유지된 민감한 신용카드 정보는 전송구간 전체에서 복호화 될 수 없으며 평문으로 존재하는 구간이 없어야한다.

☞ "민감한 신용카드 정보" 전송구간(POS 단말기 본체→VAN사 서버)의 기밀성 보증 수준

POS 단말기 본체로부터 VAN사 서버로 전송되는 구간의 기밀성 보증 수준은 다음과 같다.

① 112비트 이상의 보안강도로 암호화된 민감한 신용카드 정보는 POS 단말기와 통신하는 VAN사 서버에서만 신용카드 거래 요청의 목적으로 복호화 될 수 있다.

② 통신 중계 등을 목적으로 POS 단말기 본체로부터 VAN사 서버까지의 민감한 신용카드 정보 전송구간 상에 존재하는 어떠한 서버(예-EDI 가맹점 중계서버)도 암호화된 민감한 신용카드 정보를 복호화 할 수 없다.

5.1.2 POS 단말기는 민감한 신용카드 정보를 저장하거나 출력하지 않아야 한다.

※ 응용 시 주의사항 : 1. POS 단말기는 신용거래 승인 시 출력하는 모든 전표에 민감한 신용카드 정보를 출력하지 않아야 한다. 2. POS 단말기는 신용카드 거래 승인시점부터 민감한 신용카드 정보를 저장하지 않아야 하며 메모리에서 삭제해야 한다.

☞ 민감한 신용카드 정보의 저장 및 출력 금지

① 민감한 신용카드 정보는 카드리더기 내부에서 파일형태로 저장될 수 없으며 암호화 된 경우에도 파일형태로 저장될 수 없다.

② 민감한 신용카드 정보는 신용카드 거래 승인시점 이후 카드리더기 내부 메모리에서 완전 삭제되어야 하며 암호화된 경우에도 카드리더기 내부 메모리에서 완전 삭제되어야 한다.

③ 암호화된 민감한 신용카드 정보는 POS 단말기 본체에 파일형태로 저장될 수 없다. 단, 민감한 신용카드 정보 중 신용카드 번호는 마스킹 되어 POS 단말기 본체 내부에 파일형태로 저장될 수도 있다. (5.4 신용카드 번호 보호 참고)

④ 민감한 신용카드 정보는 신용거래 승인 시 출력하는 모든 전표에 출력될 수 없다. 단, 민감한 신용카드 정보 중 신용카드 번호는 마스킹 되어 전표에 출력될 수 있다. (5.4 신용카드 번호 보호 참고)

☆♣ "민감한 신용카드 정보 보호" 시험요구사항

개발업체는 개발한 POS 단말기가 "민감한 신용카드 정보 보호" 보안요구사항을 만족하고 있음을 증명하여야 한다. 개발업체는 암호화 대상 정보, 적용 암호알고리즘 및 카드리더기에서 VAN사까지의 암호화 방식 등을 기술한 문서를 시험기관에 제공하여야 한다. 개발업체는 해당 기능에 대한 시험 증거자료 및 추가적으로 시험기관에서 정의한 시험지원 자료를 시험기관에 제공하여야 한다.

5.2 암호 연산 및 암호키 생성/분배

민감한 신용카드 정보의 기밀성을 제공하기 위하여 사용되는 암호연산 및 암호키는 다음의 요구사항을 만족해야 한다.

5.2.1 민감한 신용카드 정보는 112비트 이상의 보안강도를 갖는 암호알고리즘과 암호키 길이에 따라 암호화 되어야 한다.

※ 응용 시 주의사항 : 민감한 신용카드 정보에 대한 암호화 시 동일한 암호문이 생성되지 않아야 한다.

☞ "112비트 이상의 보안강도를 갖는 암호알고리즘"

112비트 이상의 보안강도를 갖는 암호알고리즘 목록은 암호모듈검증 대상 보호함수(국가사이버안전센터)와 최신버전의 '암호 알고리즘 및 키길이 이용안내서(한국인터넷진흥원)'를 참고한다.

① 암호알고리즘의 보안강도란 암호 알고리즘이나 시스템의 암호키 또는 해쉬함수의 취약성을 찾아내는데 소요되는 작업량을 수치화한 것을 의미하며 112비트의 보안강도란 2^{112}번의 계산 수행을 통하여 암호키 또는 암호 알고리즘의 취약성을 알아낼 수 있음을 의미한다.

② 국내에서 권고하는 112비트 이상의 보안강도를 갖는 암호알고리즘의 목록은 다음과 같다.

1. 대칭키 암호알고리즘은 AES-128/192/256, 3TDEA, SEED, HIGHT, ARIA-128/192/256 등이다.

☞ "112비트 이상의 보안강도를 갖는 암호알고리즘"

2. 암/복호화를 위한 공개키 알고리즘은 RSAES-OAEP 2048이다.
   - o RSAES-OAEP에서 사용하는 해쉬함수는 SHA-224/256/384/512이다.
   - o HAS-160, SHA-1은 112비트에 포함되나 충돌 저항성이 112비트 보안강도를 제공하지 못하므로 사용하지 않는 것을 권장한다.
3. ECC 알고리즘은 전자서명용으로만 권고하고 있음으로, 민감한 신용카드 정보 암/복호화를 위한 공개키 알고리즘으로는 사용하지 않는 것을 권고한다.

5.2.2 안전성이 검증된 암호키 생성/분배 방법이 사용되어야 한다.

☞ "안전성이 검증된 암호키 생성/분배 방법"

안전성이 검증된 암호키 생성/분배 방법이라 함은 다음과 같다.

① 국내외 표준 또는 가이드문서 또는 보안표준에 준하는 문서 등에서 권고하고 있는 암호키 생성/분배 방법

※ "암호 알고리즘 및 키 길이 이용 안내서(한국인터넷진흥원, 2013.6.28)"에서는 공개키 기반의 키 공유 알고리즘인 DH 및 ECDH를 권고하고 있다.

※ 관련된 국외 표준 등은 ISO/IEC 11770-3(2008), PKCS#1, PKCS#3 등이 있다.

② 국내 암호모듈검증 제도에 따라 검증받은 암호키 생성/분배 방법

※ KSX ISO/IEC 19790 : 2007, 정보기술-보안기술-암호모듈보안 요구사항

③ 기타 국내외 전문기관에서 안전성을 검증 받은 암호키 생성/분배 방법

☞ "암호키 수명(생명주기)"

민감한 신용카드 정보 암호화에 사용되는 암호키는 적절한 암호키 수명(생명주기)을 가져야 한다. 적절한 암호키 수명이란 국내외 전문기관에서 권고하고 있는 암호키의 유효기간을 의미한다.

※ NIST SP 800-57(Recommendation for Key Management: Part 1 : General (Revision3), 2012.7), KISA 암호이용 안내서(2013.12) 등에서는 암호키 수명에 대한 권고사항을 기술하고 있다.

☆♣ "암호 연산 및 암호키 생성/분배" 시험요구사항

개발업체는 개발한 POS 단말기가 "암호 연산 및 암호키 생성/분배" 보안요구사항을 만족하고 있음을 증명하여야 한다. 개발업체는 사용 암호알고리즘의 보안강도, 암호키 생성/분배 방법의 안전성 근거 자료 등을 기술한 문서를 시험기관에 제공하여야 한다. 개발업체는 사용하는 암호알고리즘의 구현 적합성 관련 시험 증거자료 및 추가적으로 시험기관에서 정의한 시험지원 자료를 시험기관에 제공하여야 한다.

5.3 암호키 접근 통제 및 파기

민감한 신용카드 정보 암호키의 안전성을 보장하기 위해 다음의 요구사항을 만족해야 한다.

5.3.1 암호키에 대한 인가되지 않은 접근은 허용되지 않아야 한다.

※ 응용 시 주의사항

1. 암호키에 대한 물리적/논리적 접근은 인가된 관리자/프로그램 등에게만 허용되어야 한다.
2. 민감한 신용카드 정보 암호화를 목적으로 카드리더기에 사용되는 암호키는 안전하게 저장/관리되어야 하며, 카드리더기는 암호키에 대한 비인가된 접근시도를 방어해야 한다.

☞ "비인가된 암호키 접근시도에 대한 방어"

① 카드리더기 내부에 저장되는 암호키는 암호화되어 저장되어야 한다.

② 카드리더기는 카드리더기 외부 인터페이스(USB Port, JTAG Port 등)를 통한 카드리더기 내부에 대한 비인가된 논리적 접근 시도를 방어해야 한다.

3. 안전성이 검증된 암호키 접근통제 방법이 사용되어야 한다.

☞ "안전성이 검증된 암호키 접근통제 방법"

안전성이 검증된 암호키 접근통제 방법은 다음과 같다.

① 암호키 접근통제를 위한 스마트카드, 보안토큰과 같은 템퍼 프루프(Tamper-Proof) 매체의 사용

② 국내외 표준 또는 가이드문서 또는 보안표준에 준하는 문서 등에서 권고하고 있는 암호키에 대한 논리적/물리적 접근통제 방법

③ 기타 국내외 전문기관에서 안전성을 검증 받은 암호키 접근통제 방법

5.3.2 사용이 만료/종료된 암호키 및 암호키 생성/분배를 위해 사용된 모든 정보는 카드리더기 및 POS 단말기에서 삭제(파기)되어야 한다.

☞ "암호키 생성/분배에 사용된 정보"의 삭제

암호키 생성/분배를 위해 사용된 모든 정보란 키 길이, 키 종류, 유효기간 등을 의미하며 카드리더기 및 POS 단말기 본체에서 암호키 생성/분배를 위해 사용된 모든 정보는 사용 만료/종료된 후 삭제(파기)되어야 한다.

※ 응용 시 주의사항: 안전성이 검증된 암호키 삭제 방법이 사용되어야 한다.

☞ "안전성이 검증된 암호키 삭제 방법"

안전성이 검증된 암호키 삭제 방법 중 대표적인 예는 키를 '0' 등의 특정 문자로 채운 후 해당 메모리를 해제하는 방법이다.

☆♣ "암호키 접근통제 및 파기" 시험요구사항

개발업체는 개발한 POS 단말기가 "암호키 접근통제 및 파기" 보안요구사항을 만족하고 있음을 증명하여야 한다. 개발업체는 사용하는 암호키 접근통제 및 파기 방법, 사용 방법의 안전성 근거자료 등을 기술한 문서를 시험기관에 제공하여야 한다. 개발업체는 관련 시험 증거자료 및 추가적으로 시험기관에서 정의한 시험지원 자료를 시험기관에 제공하여야 한다.

5.4 신용카드 번호 보호

신용카드 번호를 보호하기 위하여 다음의 요구사항을 만족해야 한다.

5.4.1 신용카드 번호는 신용카드 번호 전송구간 전체에서 암호화, 마스킹, 전용망을 이용한 전송 등의 방법으로 보호되어 전송되어야 한다.

☞ "신용카드 번호"의 보호

① 보안요구사항 5.1.1에 따라 신용카드 번호는 민감한 신용카드 정보로 포함되어 암호화되고 전송보호 되어야 한다.

② '신용카드 번호'가 카드사가 승인한 매입 업무 처리, 카드사 제휴서비스 연계, 전표 출력의 목적으로 POS 단말기 본체/POS 서버 등으로 전송이 필요한 경우,
'신용카드 번호' 전체 또는 일부는 민감한 신용카드 정보와 별도로 카드리더기로부터 읽혀진 후, POS 단말기 본체/POS 서버 등으로 전송될 수 있다.
단, 추가적으로 전송되는 '신용카드 번호'는 암호화, 마스킹, 전용망을 이용한 전송 등의 방법으로 보호되어 전송구간 내에서 전송되어야 한다.

※ 응용 시 주의사항: 신용카드 번호 전송구간은 신용카드 번호가 카드리더기를 통하여 읽혀지는 시점부터 VAN사 서버로 전송되는 구간 전체를 의미한다. 각 전송구간별 신용카드 번호의 전송 보호 수준은 시험요구사항을 참조한다.

☞ "신용카드 번호" 전송구간(카드리더기→VAN사 서버)의 전송 보호 수준

추가적으로 전송되는 '신용카드 번호'에 대한 전송 보호 수준은 다음과 같다.

① 신용카드 번호가 암호화 되지 않는 무선망, 일반 인터넷 망 등 OPEN망/구간을 통하여 전송구간 내에서 전송되는 경우, '신용카드 번호' 전부는 암호화되거나 일부 마스킹되어 전송되어야 한다.

※ 'OPEN 망/구간'의 예는 다음과 같다.

1. 카드리더기와 POS단말기 본체 간 암호화되지 않은 무선 연결구간
2. 일반 인터넷 망으로 연결된 가맹점과 VAN사 또는 가맹점과 카드사 구간
3. 일반 인터넷 망으로 연결된 POS 단말기와 POS서버 구간

※ '신용카드 번호' 암호화 시, '신용카드 번호'는 카드사가 승인한 매입 업무, 카드사 제휴서비스 연계 처리 등의 목적으로 사용하는 주체의 키로 암호화될 수 있으며 112비트 이상의 보안강도를 갖는 암호알고리즘과 암호키 길이에 따라 암호화 되어야 한다.

※ '신용카드 번호' 마스킹 시, 신용카드 번호 전체 자리 중 7번째에서 12번째 번호는 '*'로 마스킹 되어야 한다.

② 신용카드 번호가 전송구간 내에서 전용망(또는 전용망으로 간주될 수 있는 전송선로)을 이용하여 전송되는 경우, 신용카드 번호는 암호화 되지 않거나 마스킹 되지 않고 전송될 수 있다.

※ '전용망(또는 전용망으로 간주될 수 있는 전송선로)'의 예는 다음과 같다.

1. 카드리더기와 POS단말기 본체 간 유선 연결구간(시리얼통신, USB연결 등)
2. POS단말기 본체와 VAN사간 전화선 연결구간
3. VPN 암호화 통신 구간
4. 전용망으로 연결된 POS단말기와 POS서버 또는 POS 단말기와 VAN사 또는 POS 단말기와 카드사 구간

☞ **"신용카드 번호" 전송구간(카드리더기→VAN사 서버)의 전송 보호 수준**

5. 전용망으로 연결된 POS서버와 VAN사 또는 POS서버와 카드사 구간

☞ **"카드사 제휴서비스 처리 방법의 예"**

① POS 단말기는 신용카드 거래를 위해 읽어온 track2 (equivalent) data 중 신용카드번호/제휴(상품)코드/OCB(OK CashBag) 구분자 등을 전송구간 내 존재하는 별도 단말기에 "신용카드 번호" 전송 보호 수준에 따라 전송한다.

② 해당 정보를 전송받은 단말기는 전송된 카드 BIN 또는 제휴(상품)코드 등을 확인하여 선할인, 포인트 적립 등 제휴서비스 업무를 처리한다.

5.4.2 신용카드 번호는 신용카드 번호 전송구간 전체에서 암호화, 마스킹, 거래를 구분할 수 있는 다른 정보로 변환 등의 방법으로 보호되어 저장되어야 한다.

☞ **"신용카드 번호"의 보호**

① 보안요구사항 5.1.1에 따라 민감한 신용카드 정보로 포함되어 암호화 된 신용카드 번호는 보안요구사항 5.1.2에 따라 신용카드 번호 전송구간 전체에서 어떠한 형태로도 저장될 수 없다.

② '신용카드 번호'가 카드사가 승인한 매입 업무 처리, 카드사 제휴서비스 연계의 목적으로 POS 서버 등에 저장이 필요한 경우,
'신용카드 번호' 전체 또는 일부는 민감한 신용카드 정보와 별도로 카드리더기로부터 읽혀진 후, POS 서버 등으로 전송된 후 저장될 수 있다.
단, 추가적으로 전송된 후 저장되는 '신용카드 번호'는 암호화, 마스킹, 거래를 구분할 수 있는 다른 정보로 변환 등의 방법으로 보호되어 저장되어야 한다.

※ 응용 시 주의사항: 1. 신용카드 번호 전송구간 내에서의 신용카드 번호 저장은 업무상 필요성이 인정되는 경우에만 허용된다. 각 전송구간별 신용카드 번호의 저장 보호 수준은 시험요구사항을 참조한다.

☞ **"신용카드 번호" 전송구간(카드리더기→VAN사 서버)의 저장 보호 수준**

추가적으로 전송된 후 저장되는 '신용카드 번호'에 대한 저장 보호 수준은 다음과 같다.

① 신용카드 번호가 전송구간 내에서 암호화 되지 않는 무선망, 일반 인터넷 망 등 OPEN망/구간을 이용하여 전송되는 경우, '신용카드 번호'는 일부 마스킹되거나, 거래를 구분할 수 있는 다른 정보로 변환되어 저장되어야 한다.
※ 'OPEN망/구간'의 예는 보안요구사항 5.4.1과 같다.
※ '신용카드 번호' 마스킹 저장 시, 신용카드 번호 전체 자리 중 7번째에서 12번째 번호는 '*'로 마스킹되어 저장되어야 한다.
※ 거래를 구분할 수 있는 다른 정보로 변환되어 저장되는 예
1. 신용카드 번호에 대한 해쉬(HASH)값. 단, 충돌 저항성이 112비트 보안강도 이상인 해쉬 알고리즘 사용 권고
2. VAN사 또는 카드사에서 거래 구분 시 사용하는 값
3. 기타 거래를 구분할 수 있는 다른 정보로 인정될 수 있는 값

② 신용카드 번호가 전송구간 내에서 전용망 (또는 전용망으로 간주될 수 있는 전송선로)을

☞ **"신용카드 번호" 전송구간(카드리더기→VAN사 서버)의 저장 보호 수준**

이용하여 전송되는 경우, 신용카드 번호는 암호화 되거나, 일부 마스킹되어 저장되어야 한다.
※ '전용망(또는 전용망으로 간주될 수 있는 전송선로)'의 예는 보안요구사항 5.4.1과 같다.
※ '신용카드 번호' 암호화 저장 시, '신용카드 번호'는 카드사가 승인한 매입 업무 처리, 카드사 제휴서비스 연계의 목적으로 사용하는 주체(예-가맹점)의 키로 암호화될 수 있으며 112비트 이상의 보안강도를 갖는 암호알고리즘과 암호키 길이에 따라 암호화 되어 저장되어야 한다. (보안요구사항 5.2 참조)
※ '신용카드 번호' 마스킹 저장 시, 신용카드 번호 전체 중 7번째에서 12번째 번호는 '*'로 마스킹되어 저장되어야 한다.

2. 저장이 허용되는 경우, 신용카드 번호는 암호화, 마스킹, 거래를 구분할 수 있는 다른 정보로 변환 등으로 보호되어 일정기간만 저장되어야 한다.

☞ **"신용카드 번호" 저장 기간**

신용카드 번호 전송구간 내에서 '신용카드 번호'가 암호화, 마스킹, 거래를 구분할 수 있는 다른 정보로 변환되어 저장할 수 있는 기간은 최대 3개월이다.

3. 저장 기간이 만료된 경우, 해당정보는 저장소에서 완전 삭제되어야 한다.

☞ **"암호화 또는 마스킹 등으로 보호된 신용카드 번호의 완전삭제"**

완전삭제의 의미는 다음과 같다.

① 완전삭제란 저장 공간(파일시스템)에 저장된 해당 정보의 기록영역을 0 또는 랜덤한 값으로 덮어쓰는 방법을 의미한다.

② 대표적인 완전삭제 방법은 DoD 5220.22-M(또는 DoD 5200.28-STD)이며, 본 요구사항에서는 최소 3회 이상의 덮어쓰기를 권고한다.

5.4.3 POS 단말기는 승인 완료된 거래에 대해 거래 종료 시점에 신용카드 번호가 더 이상 가용되지 않도록 메모리에서 삭제(파기)해야 한다.

☞ **"승인 완료된 거래의 신용카드 정보 파기"**

승인 완료된 거래란 POS 단말기로부터 요청된 신용거래가 완료되어 POS 단말기 모니터 화면의 표시 및 매출전표의 출력이 이루어진 거래를 의미한다.
POS단말기는 승인 완료 후 신용카드 번호를 메모리에서 파기해야한다.

5.4.4 신용카드 번호를 POS 단말기 모니터 화면에 표시하는 경우 신용카드 번호는 아래 "응용 시 주의사항"에 명시된 방식으로 마스킹 되어야 한다.

※ 응용 시 주의 사항: 신용카드 카드번호 전체 자리 중 7번째에서 12번째 번호는 '*'로 마스킹되어야 한다.

5.4.5 POS 단말기가 매출 전표를 출력 시 신용카드 번호는 아래 "응용 시 주의사항"에 명시된 방식으로 마스킹되어 출력하여야 한다.

※ 응용 시 주의 사항: 신용카드 카드번호 전체 자리 중 7번째에서 12번째 번호는 '*'로 마스킹되어야 한다.

☆♣ "신용카드 번호 보호" 시험요구사항

개발업체는 개발한 POS 단말기가 "신용카드 번호 보호" 보안요구사항을 만족하고 있음을 증명하여야 한다. 개발업체는 신용카드 번호 전송 보호 체계, 신용카드 번호 저장 보호 체계, 삭제 주기, 삭제 방법 메커니즘 등을 기술한 문서를 시험기관에 제공하여야 한다. 개발업체는 관련 시험 증거자료 및 추가적으로 시험기관에서 정의한 시험지원 자료를 시험기관에 제공하여야 한다.

5.5 자체보호

POS 단말기의 정상적인 동작을 보장하기 위하여 다음의 요구사항을 만족해야 한다.

5.5.1 카드리더기는 시동 시 및 [선택 : 주기적으로, 관리자 요청 시] 보안기능 실행코드 및 보안기능 관련 저장데이터(보안기능 관련 프로그램 설정값 등) 변경 여부를 탐지하기 위한 무결성 점검을 수행하여야 하며 수행결과를 관리자가 조회할 수 있어야한다.

☞ "카드리더기의 무결성 점검"

카드리더기의 무결성 점검이란 보안기능을 수행하는 카드리더기의 보안기능 실행코드, 보안기능 관련 설정 값 등의 무단 생성 및 변경, 삭제 여부를 점검함을 의미한다.

① 보안기능 관련 저장데이터는 알람 규칙, 정책 설정 등이 있으며 해당 데이터는파일시스템에 평문으로 존재할 수 없다.

② 무결성 점검을 주기적으로 수행할 시 간격은 기본적으로 설정된 시간 마다 (예 : 6시간 마다) 혹은 인가된 관리자에 의해 설정된 시간(예: 매일 특정시간)마다 수행한다.

5.5.2 카드리더기는 무결성 검증 실패 시 동작 중단 및 POS 단말기 관리자에게 해당내용을 자동으로 통보해야한다.

☞ "카드리더기의 무결성 검증 실패 시 대응 방안"

무결성 점검 결과 변조탐지 및 무결성 검증 동작 실패 시 카드리더기 동작 중단과 함께 결과를 관리자에게 경고음 또는 카드리더기 화면 출력, 카드리더기와 연결된 POS 단말기 본체 모니터 화면 출력 등으로 통보해야 한다.

☆♣ "자체보호" 시험요구사항

개발업체는 개발한 POS 단말기가 "자체보호" 보안요구사항을 만족하고 있음을 증명하여야 한다. 개발업체는 무결성 보호 대상 목록, 무결성 검사 메커니즘 등을 기술한 문서를 시험기관에 제공하여야 한다. 개발업체는 관련 시험 증거자료 및 추가적으로 시험기관에서 정의한 시험지원 자료를 시험기관에 제공하여야 한다.