모바일 후불 교통카드

성 국 큐앤솔브 부사장
박진성 스마트젠 기술연구소 이사, 연구소장

1. 머리말

2013년 12월 18일 울산광역시에 세계 최초 모바일 후불교통카드(스마트폰) 개통식이 거행되었다. 이로써 울산광역시 시민들은 선불카드 충전이나 지갑을 소지해야 하는 번거로움 없이 NFC 기능이 탑재된 스마트폰으로 버스 등 대중교통 요금을 결제할 수 있다.

본 사업은 미래창조과학부, 한국인터넷진흥원과 울산광역시가 2013년 1월 협약을 체결하고 추진하였으며, 한국무선인터넷산업연합회, 이동통신사(SKP, KT, LGU+), 신용카드사(신한카드, KB국민카드, 롯데카드, 비씨카드), 교통카드사(이비카드, 마이비), 울산광역시 버스운송사업조합 등 13개사가 참여하였다.

코리아NFC표준화포럼에서는 본 사업의 추진을 위해서 모바일 후불교통카드 관련 개발 규격을 표준화함으로써, 모바일 교통 결제 서비스의 활성화를 도모하고 모바일 선불 및 후불결제 수단을 통합 관리하는 애플릿을 통해서 사용자의 교통 결제 수단에 대한 선택권을 제공할 수 있으며, 이를 통해 표준화된 지불 결제 방식을 수행할 수 있어 NFC 서비스의 호환성 및 인프라 확대를 기대할 수 있게 되었다.

본 표준은 콤비 USIM 또는 NFC USIM에 탑재되는 후불 교통카드 서비스를 위한 애플릿과 모바일 선불 및 후불 교통 결제 수단을 관리하는 애플릿에 대한 규격을 정의하고 있다. 본 표준에서 정의하는 애플릿은 콤비 USIM 및 NFC USIM에 탑재되어 교통 결제 서비스를 수행할 수 있도록 설계되었으며, 통합 결제 서비스에 참여하는 구성 요소(단말, 정산 시스템 등) 간 상호 호환성이 보장되도록 설계되었다.

본 고에서는 금번 제정된 모바일 후불 교통 카드 표준 관련 정의 및 특성에 대해서 설명하고 표준의 주요 내용인 모바일 후불 파일 시스템, 보안 메커니즘, 명령어, 프로토콜 등에 대한 구체적인 표준 항목에 대한 개략적인 설명을 통해 표준의 필요성과

<표 1>

INS	명령어	내용
A4	Select File	Config DF 애플릿을 선택한다. 후불 교통 서비스 애플릿에 관한 정보를 얻기 위해 필히 수행되어야 한다.
B2	Read Record	지정된 파일의 Record에 저장된 데이터를 읽는다.
CA	Get Data	카드로부터 AppCode(Application Code) 또는 EFconfig list 잔여 개수를 획득한다.
82	External Auth	지정된 키를 이용하여 외부 인증을 획득한다.
50	Initialize Update	External Auth 명령을 수행하기 전에 수행되어야 하는 명령으로 내부에 Session Key를 생성하고 상호 인증하기 위해 초기화를 수행한다.
20	Verify PIN	PIN1 또는 PIN2 인증을 한다.
24	Change PIN	PIN1 또는 PIN2 data 갱신한다.
42	Read List	지정된 AID의 EFconfig list read한다
44	Update List	지정된 AID의 EFconfig list Update한다
46	Delete List	지정된 AID의 EFconfig list를 delete한다
48	Update EFconfig	지정된 AID의 EFconfiglist data를 EFconfig로 update한다.

우수성을 논하고자 한다.

2. 주요 내용

본 표준은 모바일에서 후불로 교통카드 결제에 필요한 물리적인 요구사항으로 ISO/IEC 14443을 준용하고 있으며, ISO/IEC 7816에 따른 파일 시스템, 그리고 Triple DES 또는 SEED 알고리즘을 이용한 보안 메커니즘 등을 규정하고 있다. 추가로 USIM에서 선불 또는 후불 교통 결제 수단을 관리하는 Config DF 애플릿의 명령어 및 파일 구조와 후불 교통 서비스를 위한 모바일 후불 교통 카드 애플릿의 명령어 및 파일 구조를 정의한다.

모바일에서 교통 결제 수단을 관리하는 애플릿인 Config DF 애플릿은 다수의 교통 결제 수단이 하나의 USIM에 사용되는 모바일 환경의 특징을 반영하였다. 이동통신사별로 상이한 접근 조건을 적용 가능하도록 하기 위하여 키와 2개의 핀을 이용하여 다양한 설정이 가능하다. 결제에 사용되는 하나의 애플리케이션 정보만 저장하고 있던 기존의 Config DF와는 다르게 사용 가능한 모든 교통 호환용 애플리케이션에 대한 목록 정보를 EFCONFIG_LIST 파일에 저장하고 있으며 사용자 또는 관리자의 설정에 의해서 EFCONFIG 파일 결제에 사용되는 애플리케이션을 지정할 수 있다. 자세한 명령어는 〈표 1〉에 표시하였다.

국토해양부가 주관하는 전국호환 교통카드 표준은 선불 및 후불에 대한 거래 명령어와 거래 프로세스를 정의하고 있다. 후불 교통 서비스 애플릿은 이중에 후불 거래에 필요한 거래 명령어와 후불거래 프로토콜 및 직전 후불 거래 취소 프로토콜을 기반으로 하였으며, 여러 이동통신사와 신용카드사에서 함께 사용 가능하도록 하고, 편의성 및 서비스 연계를 지원하고, 향후 교통정책의 반영을 고려하였다.

후불 교통 서비스 애플릿은 이동통신사 및 신용카드사에서 많이 사용하는 Security Domain을 이용하여 발급 및 인증에 필요한 키를 관리하고, Security Domain Service를 이용하여 인증, 암호화, 발급 프로세스를 수행한다. 이로써 후불 교통 서비스 애플릿의 발급 및 인증이 교통카드사와 상관없이 이동통신사 독립적으로 서비스가 가능하며,

<표 2>

INS	명령어	명령어 설명
A4	Select File	후불 교통 서비스 애플릿을 선택하여 교통서비스 명령이 실행 가능하도록 한다.
C0	Get Response	카드로부터 전송되지 않은 데이터를 획득한다.
84	Get Challenge	카드로부터 난수(Random Number)를 획득한다.
82	External Auth	지정된 키를 이용하여 외부 인증을 획득한다.
50	Initialize Update	External Auth 명령을 수행하기 전에 수행되어야 하는 명령으로 내부에 Session Key를 생성하고 상호 인증하기 위해 초기화를 수행한다.
12	Issue Card	카드 발급 정보 저장
CA	Get Data	카드로부터 CSN(Chip Serial Number) 또는 AppCode(Application Code)를 획득한다.
B0	Read Binary	지정된 Binary 파일에 저장된 데이터를 읽는다.
D6	Update Binary	지정된 Binary 파일에 데이터를 갱신한다.
B2	Read Record	지정된 파일의 Record에 저장된 데이터를 읽는다.
DC	Update Record	지정된 파일의 Record의 데이터를 갱신한다.
E2	Append Record	지정된 파일에 새로운 Record를 추가한다.
4C	Read Balance	전자지갑 파일의 누적 거래 금액 정보를 읽어온다.
30	Block	현재 선택된 DF의 동작을 정지한다.
32	Unblock	현재 정지된 DF를 동작시킨다.
E8	SetLifeCycle	Life Cycle 변경하여 사용상태로 설정한다. 이 명령 실행 전에는 교통서비스 명령의 실행이 불가능하다.
02	INITIALIZE CARD	KS X 6924 후불 거래, 취소 거래를 수행하기 위한 초기화 명령어로 후불 거래 및 취소 거래를 위해 선행되어야 한다.
04	PURCHASE CARD	KS X 6924 후불 거래, 취소거래를 수행하여 잔액을 변경하고 거래 로그 등을 카드에 기록한다.

이로 인해 교통카드사 별로 필요했던 인증 및 발급용 키를 이동통신사와 신용카드사가 여타의 모바일 애플릿용 키와 같이 관리할 수 있게 하여 이동통신사 및 신용카드사의 편의성을 도모하였다.

파일 구조로는 인증용 키 파일, Purse Key 파일, 전자지갑 관리에 필요한 전장지갑 정보 파일, 환승 관련 로그 정보를 기록하는 환승 정보 내역 파일, 잔액 및 거래 내역이 저장되는 전자지갑 파일, 신용카드사 정보를 저장하는 정보파일, 유통용 데이터 파일을 정의하고 있다. 자세한 명령어는 〈표 2〉에 표시되어 있다.

신용카드사에서 필요로 하는 정보를 저장할 수 있는 공간을 별도로 마련하여 신용카드 상품 관련 정보와 멤버십 관련 정보를 저장할 수 있도록 하였고 유통 서비스 확장이 가능하도록 유통 관련 데이터 파일과 이를 관리하는 권한을 가진 키를 별도로 부여하여 제휴 서비스가 가능하도록 고려하였다.

3. 맺음말

서두에 언급한 것과 같이 세계 최초 모바일 후불교통카드 시범서비스가 울산광역시에서 시범적 으로 운영되고 있으며, 관련한 개발 규격에 대한 표준까지 제정이 완료되었다. 이는 모바일 후불 교통 카드 본 서비스를 위한 첫걸음에 지나지 않는다. 금번 제정된 표준이 많이 활용되고 모바일 후불 교통 카드 서비스가 활성화되기 위해서는 많은 부분에서 추가적인 노력이 필요한 상황이다.

이용자가 쉽게 모바일 후불 신용카드를 스마트폰에 다운 받을 수 있는 구조가 세팅이 되어져야 하며, 발급 신용카드를 교통카드 결제 외에 다양한 곳에서 기존의 플라스틱 신용카드와 마찬가지로 사용할

수 있는 결제 인프라의 보급도 시급하다.

그리고 금번 표준으로 울산 지역뿐만이 아닌 전국 호환이 될 수 있는 교통 카드 인프라 개선도 선행돼야만 모바일 후불 교통 카드 활성화를 기대할 수 있을 것이다. 그럼에도 불구하고 첫걸음을 뗐다는 부분은 상당한 의미가 있다고 판단되며 금번 제정된 표준은 향후 모바일 후불 교통카드 활성화의 큰 주축이 될 것이다. TTA

정보통신 용어해설

회전 정렬 오차 Rotational alignment error [방송]

바르게 정렬된 카메라의 광축과 비교하여 다른 카메라의 광축이 시계방향 또는 반시계 방향으로 회전이 되어 있는 상태로 촬영을 하여 생기는 좌우 영상 간의 오차.