한국항행학회 논문지 제11권 제3호 2007년 9월

비접촉식 도로통행료 징수를 위한 전자 신용카드 처리 방법

Electronic Credit Card Processing Methods for Contactless Toll Collection

박진성*, 권병헌*

Jin-Sung Park*, Byeong-Heon Kwon*

요 약

본 논문에서는 현재 국내 ETCS(Electrical Toll Collection System)에 적용될 예정에 있는 후불식 지불 방식에 있어서 수행해야할 전자 신용카드(EMV) 처리절차를 제안한다. 현재 국내에서는 한국도로공사의 하이패스, 터치패스 시스템이 비접촉식 ETCS로 운영되고 있으며, 현재의 운영 방식은 일종의 전자화폐 개념의 선불(pre-paid)식이다. 이에 반해 후불(credit)식은 신용카드 기반의 지불을 수행함으로써 미리 지불할 필요가 없다는 장점이 있다. 현재 국내의 ETCS에 후불식의 도입이 준비 중에 있으며, 본 논문에서는 이러한 후불식 지불에서 고려해야 할 EMV 처리 방식을 제안한다.

Abstract

This paper proposes Electronic Credit Card(EMV) processing procedures for a credit payment method which can be applied to Korean ETCS(Electrical Toll Collection System). In Korea, Korea Highway Corporation services contactless ETCS's called by Hi-Pass and Touch-Pass system at present. These systems operate on a pre-paid payment method similar to electronic money. On the other side, a credit payment method based on credit card has an advantage which does not require pre-paid. The introduction of credit payment method to ETCS is in preparation. In this paper, we propose EMV processing methods based on a credit payment method which can be applied on ETCS.

Key words : ETCS, EMV, contactless ETCS

I. 서 론

현재 국내에서는 스마트카드를 이용한 한국도로공사의 하이패스, 터치패스 시스템이 비접촉식 ETCS(Electrical Toll Collection System)로 운영되고 있으며, 현재의 운영 방식은 선불(pre-paid)식이다. 선불식은 일종의 전자화폐로써 스마트카드에 미리 지불한 금액을 저장하고 그 카드를 OBU(On Board Unit)에 삽입한 후 하이패스 차로를 통과하면 OBU와 RSE (Road Side Equipment) 사이의 통신을 통해 통행료가 차감되는 방식이다. 그러나 이 방식은 사용 전에 미리 일정 금액을 충전해 두어야하는 불편함이 있다. 이에 반해 후불(credit)식은 전자 신용카드 기반의 지불을 수행함으로써 미리 지불할 필요가 없다는 장점이 있다. 후불식 처리는 크게 인증식과 EMV(Europay, Master, Visa) 방식으로 구분할 수 있는데, 인증식은

* 유한대학 정보통신과(Department of Information & Communication, Yuhan College)
· 제1저자 (First Author) : 박진성
· 접수일자 : 2007년 5월 23일

카드일련번호(CSN)를 이용하여 카드 사용자를 식별하고 신용카드사에 그 금액을 청구하는 방식으로 국내에서 교통카드 분야에 적용되고 있다. EMV 방식은 비자-마스터 카드의 공통 스마트카드형 신용카드 규격인 EMV 규격에 따라 데이터를 교환하고 거래 인증을 수행하는 방식이다[1]. 현재 국내의 ETCS에 후불식의 도입이 준비 중에 있으나, 기존의 EMV 처리방식은 고속의 처리가 요구되는 도로통행료 징수에는 적합하지 않으며, 본 논문에서는 이러한 후불식 지불에서 고려해야 할 처리 속도에 중심을 둔 EMV 처리 방식을 제안한다.

Ⅱ. 일반적인 EMV 처리

2-1 일반적인 온라인 EMV 처리 절차

일반적인 온라인(online) EMV 거래는 현재의 자기띠(magnetic-strip) 기반의 신용카드 거래/승인 처리 절차를 스마트카드에 도입하여 보안에 중점을 둔 거래 절차이다.

그림 1에 나타나 있듯이 EMV 스마트카드가 EMV 신용카드 단말기에 삽입되면 EMV에 규정된 GetProcessing Option 등의 명령을 이용하여 카드로부터 거래에 필요한 데이터를 읽어오게 된다. 이 데이터로부터 거래에 적절한 신용카드인 것이 판명되

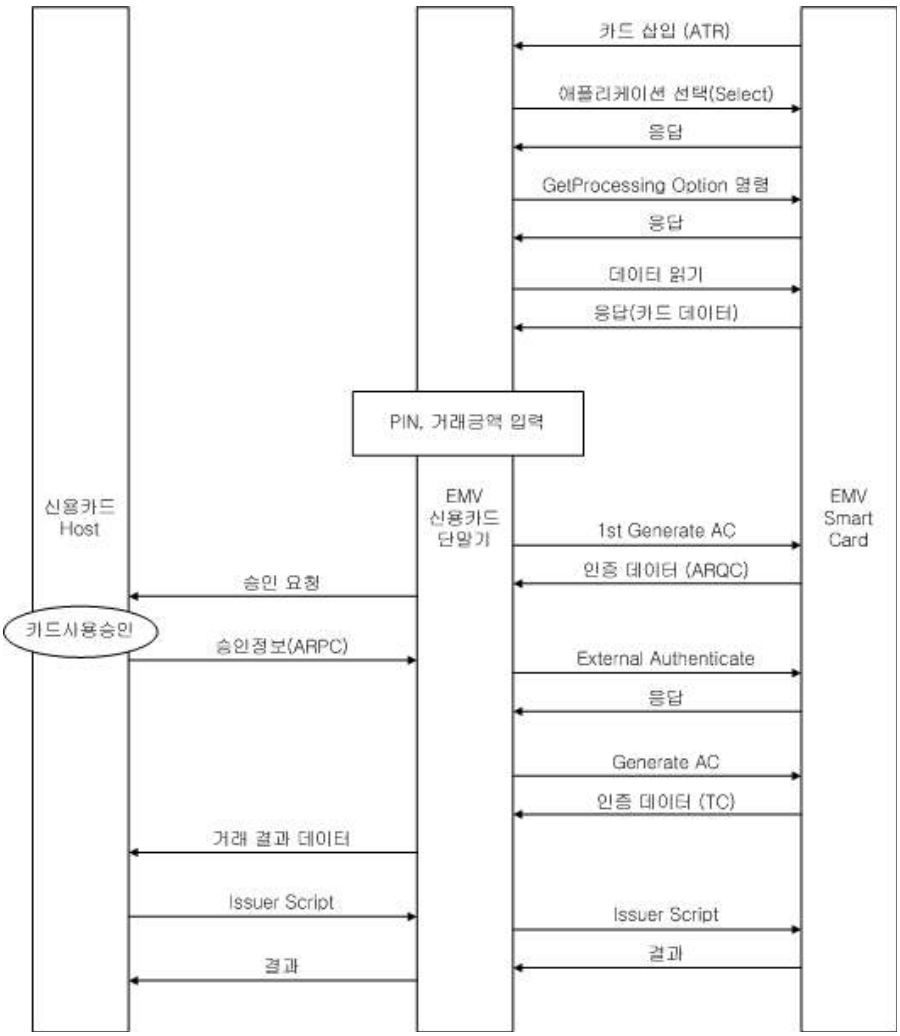

그림 1. 온라인 EMV 처리
Fig. 1. Online EMV Processing

면, 단말기는 카드비밀번호(PIN), 거래 금액 등을 입력받고 카드에 첫 번째 Generate AC 명령을 보내 거래에 필요한 암호화 인증 데이터(ARQC : Authorization Request Cryptogram)를 카드가 생성하게 하고, 이를 받아 승인 요청 데이터를 구성하여 신용카드 호스트로 전송한다. 신용카드 호스트는 이 요청 데이터를 검토하고 거래를 승인하는 암호화 데이터(ARPC : Authorization Response Cryptogram)를 생성하여 단말기로 전송한다. 신용카드 단말기는 승인 데이터를 수신하면 스마트카드에게 External Authenticate 명령과 두 번째 Generate AC 명령을 전송한다. 스마트카드가 두 번째의 Generate AC 명령의 응답으로 TC(Transaction Certificate)를 보내오면 이 거래는 성공적으로 완료된 것이다. 거래 완료 후 스마트카드에 저장된 데이터를 변경하는 것이 필요한 경우에 신용카드 호스트로부터 Issuer Script가 전송되기도 한다.

2-2 일반적인 오프라인 EMV 처리 절차

오프라인(off-line) 처리는 신용카드 단말기가 신용카드 호스트로부터 사용 승인을 받지 않아도 거래가 가능한 처리 절차이다. 이때에는 신용카드 호스트와의 통신이 없고 단말기와 카드간의 인증 정보만으로 거래가 이루어지기 때문에 처리 시간이 적게 걸린다는 장점이 있다.

EMV 스마트카드가 EMV 신용카드 단말기에 삽입되면 EMV에 규정된 GetProcessing Option 등의 명령을 이용하여 카드로부터 거래에 필요한 데이터를 읽어오게 된다. 이 데이터로부터 거래에 적절한 신용카드인 것이 판명되면, 단말기는 카드비밀번호(PIN), 거래 금액 등을 입력받고 카드에 첫 번째 Generate AC 명령을 보내 오프라인 거래를 수행할지 여부를 묻게 되고 카드가 오프라인 처리에 동의하면 스스로 인증 데이터(TC)를 생성하여 응답한다. 신용

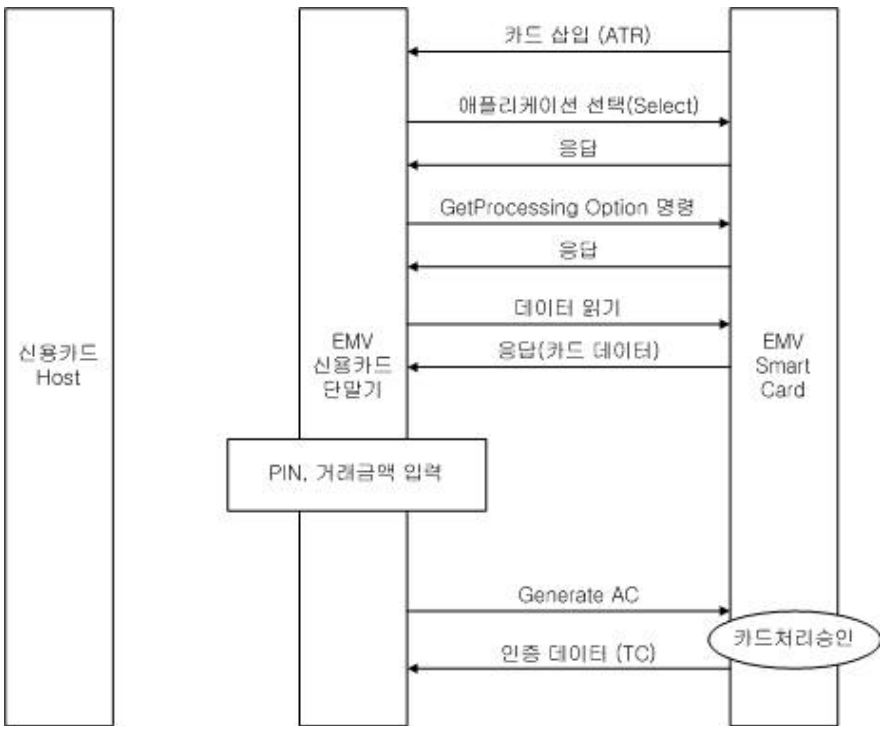

그림 2. 오프라인 EMV 처리
Fig. 2. Off-line EMV Processing

카드 단말기는 이 인증 데이터와 거래 관련 데이터를 저장하였다가 나중에 신용카드 호스트에 전송하게 된다.

Ⅲ. ETCS에서의 EMV 처리

3-1 ETCS를 위한 온라인 EMV 처리

국내에서 서비스 중인 ETCS에 EMV 거래 처리를 도입하기 위해서는 OBU와 RSE 간의 통신, 데이터 교환 규격, RSE와 호스트의 통신 등은 물론 다중 서비스 제공자, 다중 신용카드 호스트와의 연계 등 여러 가지 기술적, 정책적 문제가 존재하지만, 본 논문에서는 가장 핵심이 되는 EMV 거래 절차 부분에 중점을 두고 살펴보고자 한다.

먼저, OBU는 EMV 스마트카드가 삽입되면 카드 내의 적절한 데이터를 읽어 거래에 필요한 정보를 수집하고 자신의 메모리에 저장해 둔다. OBU가 RSE와의 통신 가능 영역에 들어오면 RSE가 발산하는 BST (Beacon Service Table) 신호를 받게 되며, 이에 대한 응답으로 VST (Vehicle Service Table)를 RSE로 전송한다. 이어 RSE는 카드와 OBU에 대한 정보를 요청하며(Get Request), 필요한 데이터를 OBU로부터 받아 과금할 금액을 결정한다.

RSE는 과금 금액과 기타 정보를 담아 Payment

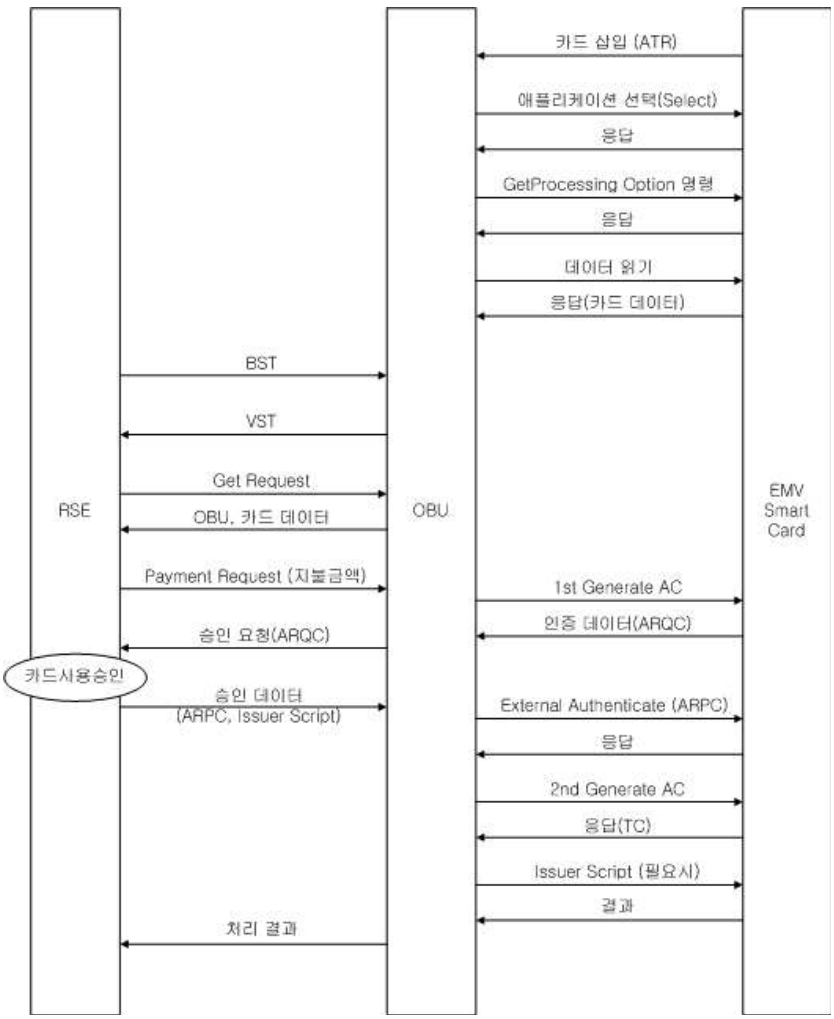

그림 3. ETCS를 위한 온라인 EMV 처리
Fig. 3. Online EMV Processing for ETCS

Request 명령을 보내고, 이를 수신한 OBU는 스마트카드에 첫 번째 Generate AC 명령을 전송한다. 이에 대한 응답으로 스마트카드가 생성한 암호화된 인증 데이터(ARQC)를 받아 카드 정보, 단말기 정보 등을 포함한 승인 요청 데이터를 구성하여 RSE로 전송한다. RSE는 요청 데이터를 분석하여 올바른 신용카드인지 확인하고 사용 한도가 적정하면 암호화된 승인 데이터 (ARPC)를 생성하여 OBU로 전송한다. 또, 카드 데이터의 변경이 필요한 경우에 Issuer Script를 포함하여 전송한다.

본 절에서는 RSE가 신용카드 호스트의 역할을 수행한다고 가정하고 그림 3의 흐름도를 구성하였는데, 그렇지 않은 경우에는 RSE가 OBU로부터 받은 ARQC 정보를 신용카드 호스트로 전송하고 신용카드 호스트가 EMV 거래 승인여부를 판단한 다음, 그 응답으로 ARPC를 RSE로 전송하면 RSE는 이것을 받아 OBU로 전송하게 된다.

OBU는 승인정보를 수신하고 이를 기반으로 스마트카드에 External Authenticate 명령과 두 번째 Generate AC 명령을 전송한다. 스마트카드가 응답으로 인증 데이터(TC)를 응답하면 거래가 성공적으로 완료된 것으로, 승인정보에 Issuer Script가 포함되어 있는 경우 이를 스마트카드로 전송하여 수행한다. 마지막으로 OBU는 처리 결과를 RSE로 전송하고 거래를 마친다.

3-2 ETCS를 위한 오프라인 EMV 처리

OBU는 스마트카드가 삽입되면 카드 내의 적절한 데이터를 읽어 거래에 필요한 정보를 수집한다. 오프라인 처리를 위해서는 이 단계에서 카드와 OBU는 서로의 데이터를 분석하여 EMV에 규정된 오프라인 처리를 수행할 준비를 한다.

OBU가 RSE와의 통신 가능 영역에 들어오면 RSE가 발산하는 BST 신호를 받게 되며, 이에 대한 응답으로 VST를 RSE로 전송한다. 이어 RSE는 카드와 OBU에 대한 정보를 요청하며(Get Request), 필요한 데이터를 OBU로부터 받아 과금할 금액을 결정한다.

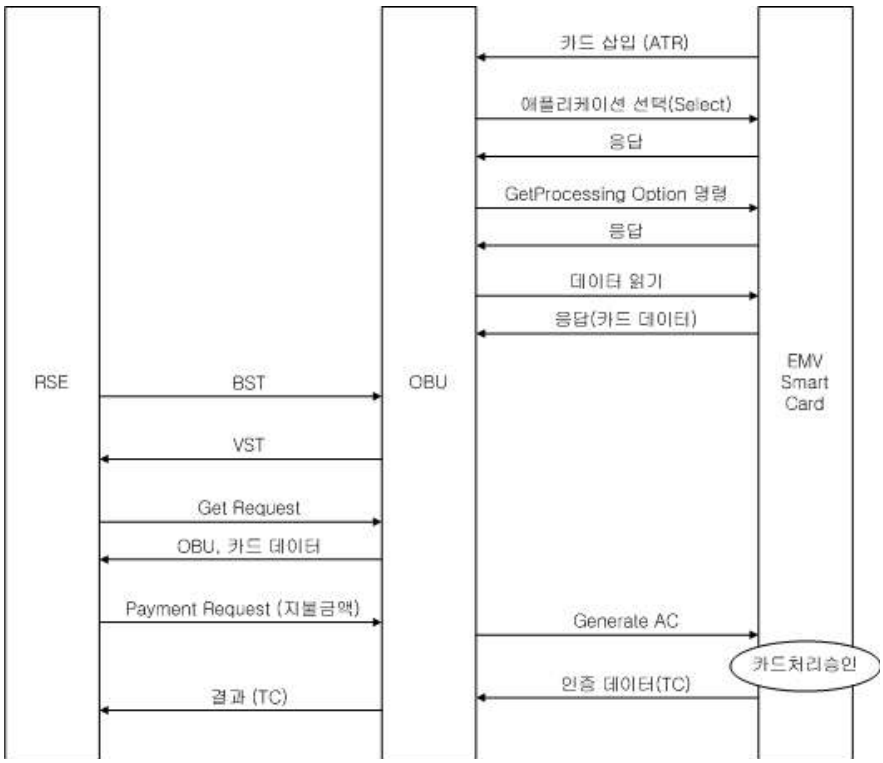

그림 4. ETCS를 위한 오프라인 EMV 처리
Fig. 4. Off-line EMV Processing for ETCS

RSE는 과금 금액과 기타 정보를 담아 Payment Request 명령을 보내고, 이를 수신한 OBU는 스마트카드에 Generate AC 명령을 스마트카드에 전송한다. OBU는 스마트카드가 생성한 암호화된 인증데이터(TC)를 받아 카드 정보, 단말기 정보 등을 포함한 거래 결과 데이터를 구성하여 RSE로 전송한다.

Ⅳ. 결 론

현재 국내에서는 한국도로공사의 하이패스, 터치패스 시스템이 비접촉식 ETCS로 운영되고 있으며, 현재의 운영 방식은 선불(pre-paid)식이다. 그러나 선불 방식은 사용 전에 미리 일정 금액을 충전해 두어야하는 불편함이 있다. 이에 반해 신용카드 기반의 후불식은 미리 충전할 필요가 없다는 장점이 있다. 후불식 처리는 크게 인증식과 EMV(Europay, Master, Visa) 방식으로 구분할 수 있는데, 본 논문에서는 이러한 후불식 지불에서 고려해야 할 EMV 처리 방식을 제안한다. 이를 위해 ETCS가 아닌 일반적인 구매 거래에서의 EMV 처리 절차를 살펴보고, 온라인 처리와 오프라인 처리를 구분하여 분석하였다. 이러한 일반 EMV 거래를 ETCS에 적용하였을 때 필요하게 되는 처리 절차를 추가하고 ETCS를 위한 EMV 온라인 / 오프라인 처리 절차를 제안하였다. 이러한 ETCS용 처리절차는 일반 처리절차에 비해 미리 데이터를 읽어두거나 우선처리할 수 있는 절차를 미리 진행해두어 차량이 톨에 진입함과 동시에 빠른 후처리를 수행함으로써 처리속도를 향상하는데 중점을 두었다.

참 고 문 헌

[1] EMVCo,LCC, “EMV2000 Integrated Circuit Card Specification for Payment Systems", *EMVCo,LCC,* Version 4, 2000.

[2] 박진성, 최명렬, “고기능 RFID 태그를 위한 동적 ID 할당 프로토콜”, *한국정보보호학회 논문지,* 제15권 제6호, pp. 49-58, 2005.

박 진 성 (朴鎭成)

1995년 2월 : 한양대학교 제어계측공학과(공학사)
1997년 2월 : 한양대학교 제어계측공학과(공학석사)
2006년 2월 : 한양대학교 제어계측공학과(공학박사)
2000년 ~ 2002년 : (주)마니네트웍 개발팀장
2003년 ~ 2004년 : 노틸러스효성(주) 개발팀 과장
2005년 5월 ~ 2007년 2월 : (주)씨이엔 연구소장
2007년 3월 ~ 현재 : 유한대학 정보통신과 강의전담교수
관심분야 : 스마트카드, RFID, 정보보호

권 병 헌 (權炳憲)

1987년 : 한국항공대학교 항공전자공학과 (공학사)
1989년 : 한국항공대학교 대학원 항공전자공학과 (공학석사)
1995년 : 한국항공대학교 대학원 전자공학과 (공학박사)
1989년 ~ 1997년 : (주)LG전자 선임연구원
현재 : 유학대학 정보통신학과 부교수
관심분야 : 영상신호처리, 통신, 3D displays.