EMV Module Security

2025.07.25

Duali

목차

- KEY 구성
- DUKPT (Derived Unique Key Per Transaction)
- Key Bundling
- Key Download를 위한 상호 인증
- Data Encrypt

KEY 구성(1)

PHASE	Private RSA Key(man)	Public RSA Key(man)
생성자	Acquirer	Acquirer
저장 위치	HOST	Reader (출고 전에 넣어져 있어야 함)
사용	Using Key 를 주고 받기 위한 상호인증용 데이터 암호화 및 사인에 사용	Using Key 를 주고 받기 위한 상호인증용 데이터 복호화 및 검증에 사용
사용자	Acquirer	Reader
수명(Life Cycle)	영구	영구
KEY 종류	RSA 2048 (256Byte)	RSA 2048 (256Byte)

Manufacturer Public RSA Key(PK(man))는 Manufacturer Room 처음 리더기 만들 시 주입(Key는 VAN에서 제공)

KEY 구성(2)

PHASE	Encryption Key
생성자	Acquirer
저장 위치	Reader
사용	데이터 전송 시 사용하는 암호화 키 생성 및 사용
사용자	Reader
KEY 사용 방식	DUKPT(ANSI X9.24-1)
키 생성에 사용되는 데이터	KSN(Key Serial Number), REG(Key 저장 IDX) PEK(Initial Key)
생성 키 데이터	21쌍의 Future Keys
수명(Life Cycle)	VAN 업데이트 주기에 따름
KEY 종류	AES 128(16Byte), TDEA(24Byte), SEED(16Byte), HIGHT(8Byte), ARIA 128(16Byte)

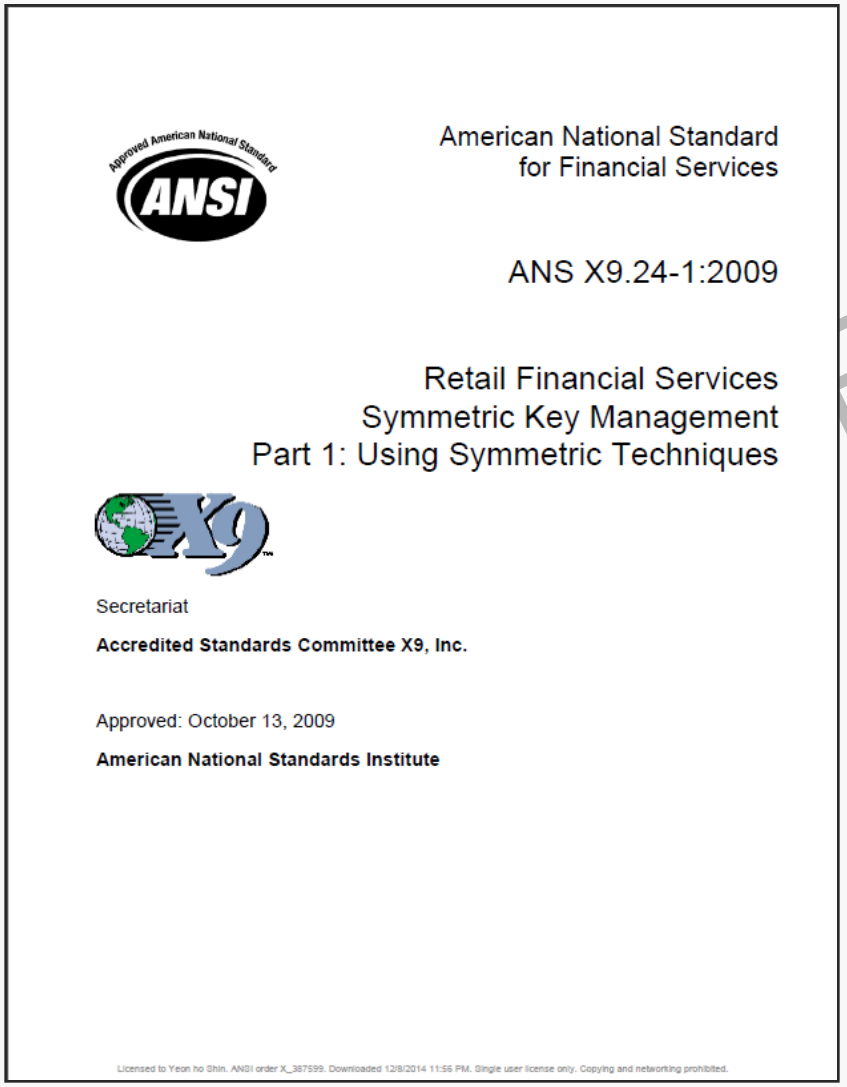
Encryption Key는 VAN에서 리더기 별로 각 각 다른 키를 생성하여, 온라인 인증을 거쳐서 리더기에 주입

KEY 구성(3)

PHASE	Transport Key(for Key Bundling)	Offline F/W Download Key
생성자	Reader(Encrypt Key 전송 상호 인증 시, Random 생성)	Acquirer
저장 위치	저장 안함	Reader의 Secure Memory
사용	Using Key Bundling	Offline F/W 다운로드 시 사용
사용자	Reader to HOST, HOST to Reader	Reader to Download Program, Download Program to Reader
수명(Life Cycle)	매 트랜잭션	영구
KEY 종류	AES 128 (16Byte 사용)	AES 128 (16Byte 사용)

Transport Key 는 상호인증 과정 후에, 실제 Using Key를 암/복호화 하여, 통신 상에 드러나지 않도록 하는 키로 사용

DUKPT(1)



American National Standard
for Financial Services

ANS X9.24-1:2009

Retail Financial Services
Symmetric Key Management
Part 1: Using Symmetric Techniques

Secretariat

Accredited Standards Committee X9, Inc.

Approved: October 13, 2009

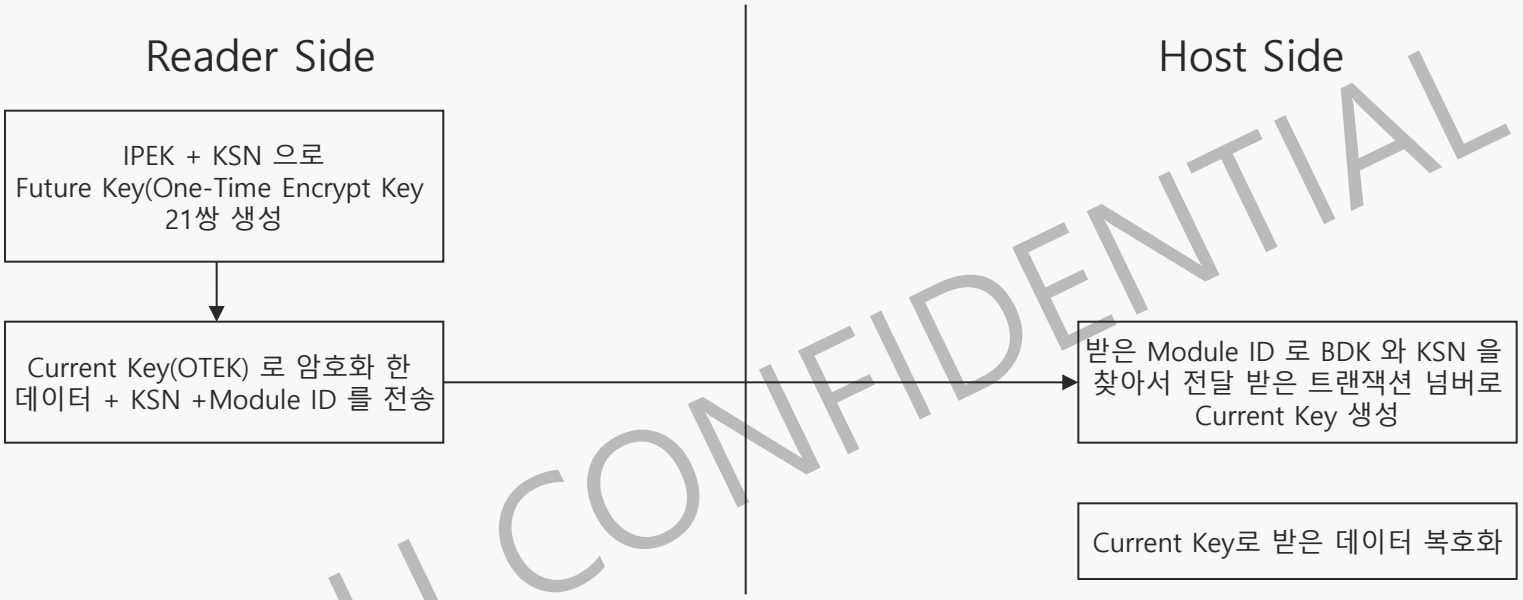
American National Standards Institute

DUKPT 방식에 대한 구현 방법 및 알고리즘(ANSI X9.24-1)

DUKPT(2)

IPEK는 처음 리더기에 Key Download 하는 시점에 Host에서 생성하거나, 또는 미리 해당 리더기 별로 Host에 생성해 놓고 사용

DUKPT(3)



받은 IPEK + KSN 을 통해 Future Key를 21쌍 리더기에 생성하여 가지고 있으며, 매 트랜잭션 후 업데이트를 함.

DUKPT(4)

Host Side

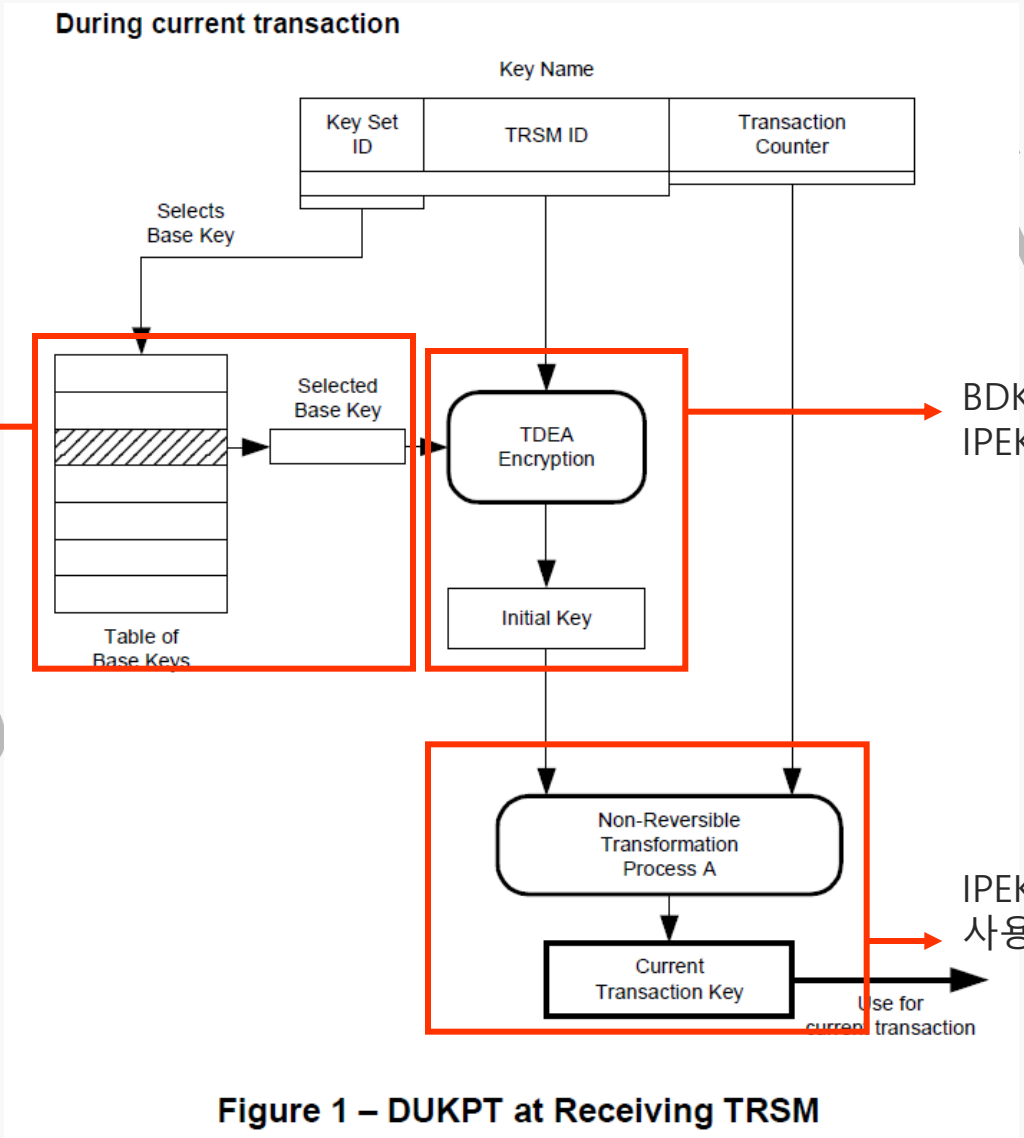


Figure 1 – DUKPT at Receiving TRSM

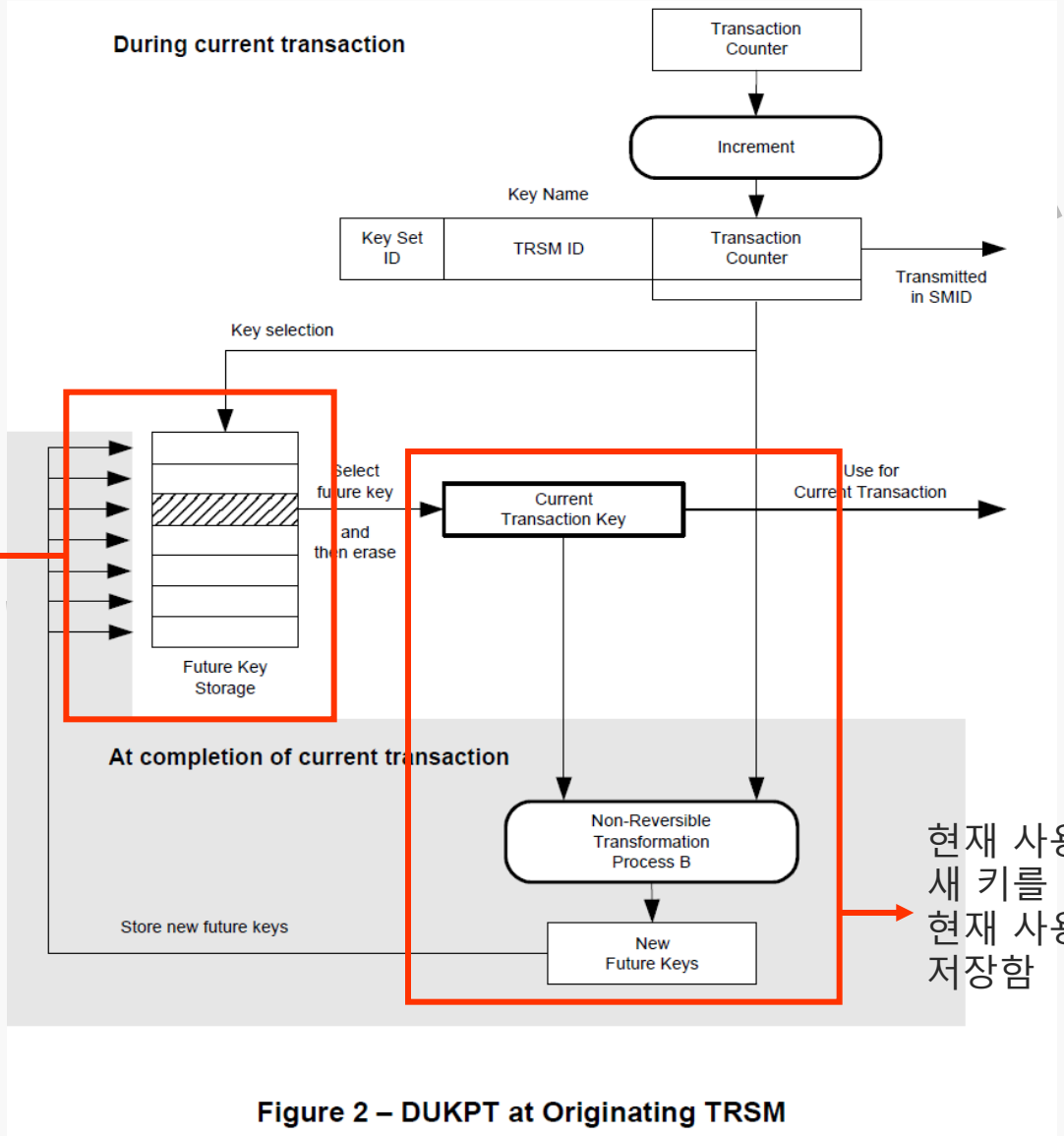
저장된 BDK 중 현재 Module ID에 해당 하는 것으로 선택

BDK, KSN 을 통해 IPEK를 처음 생성

IPEK 를 KSN 으로 현재 사용한 키를 생성

DUKPT(5)

Reader Side

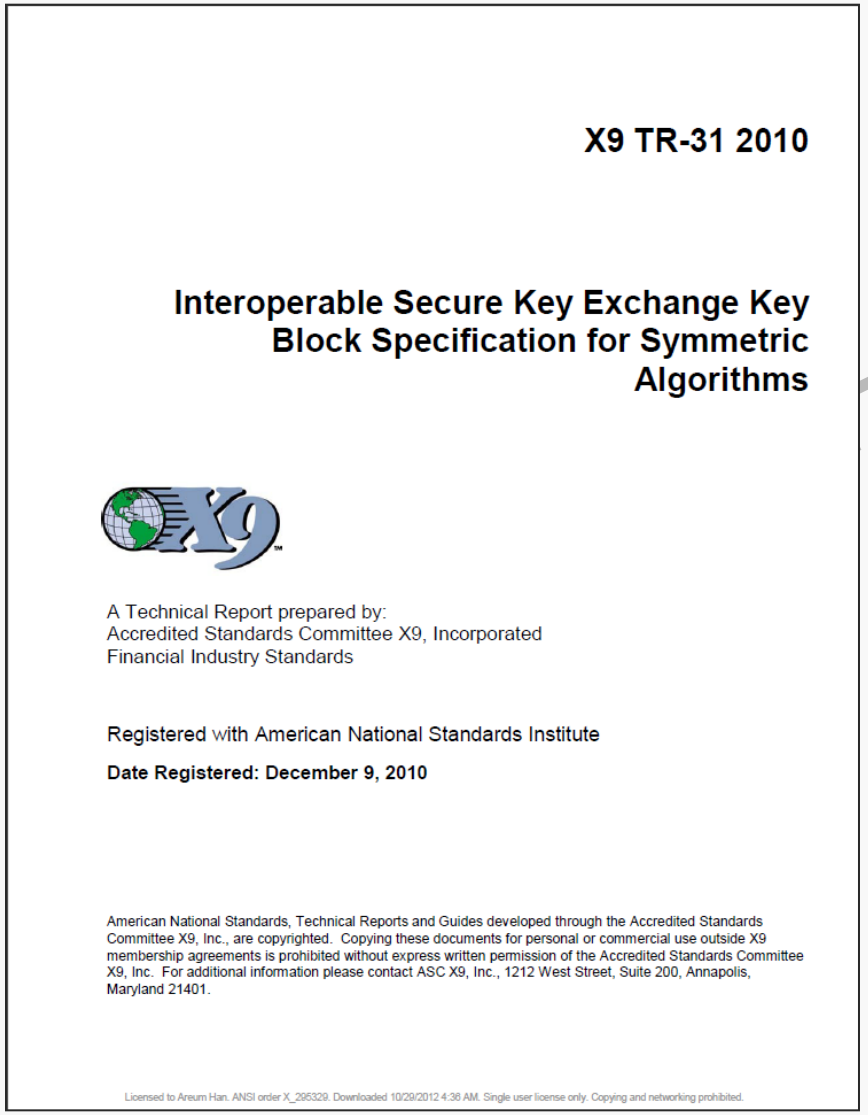


21쌍의 키를 만들어 저장해 놓고 있음

현재 사용한 키를 이용하여 새 키를 만들고, Key Store에 현재 사용한 키 위치에 새 키를 저장함

Figure 2 – DUKPT at Originating TRSM

Key Bundling



X9 TR-31 2010

Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

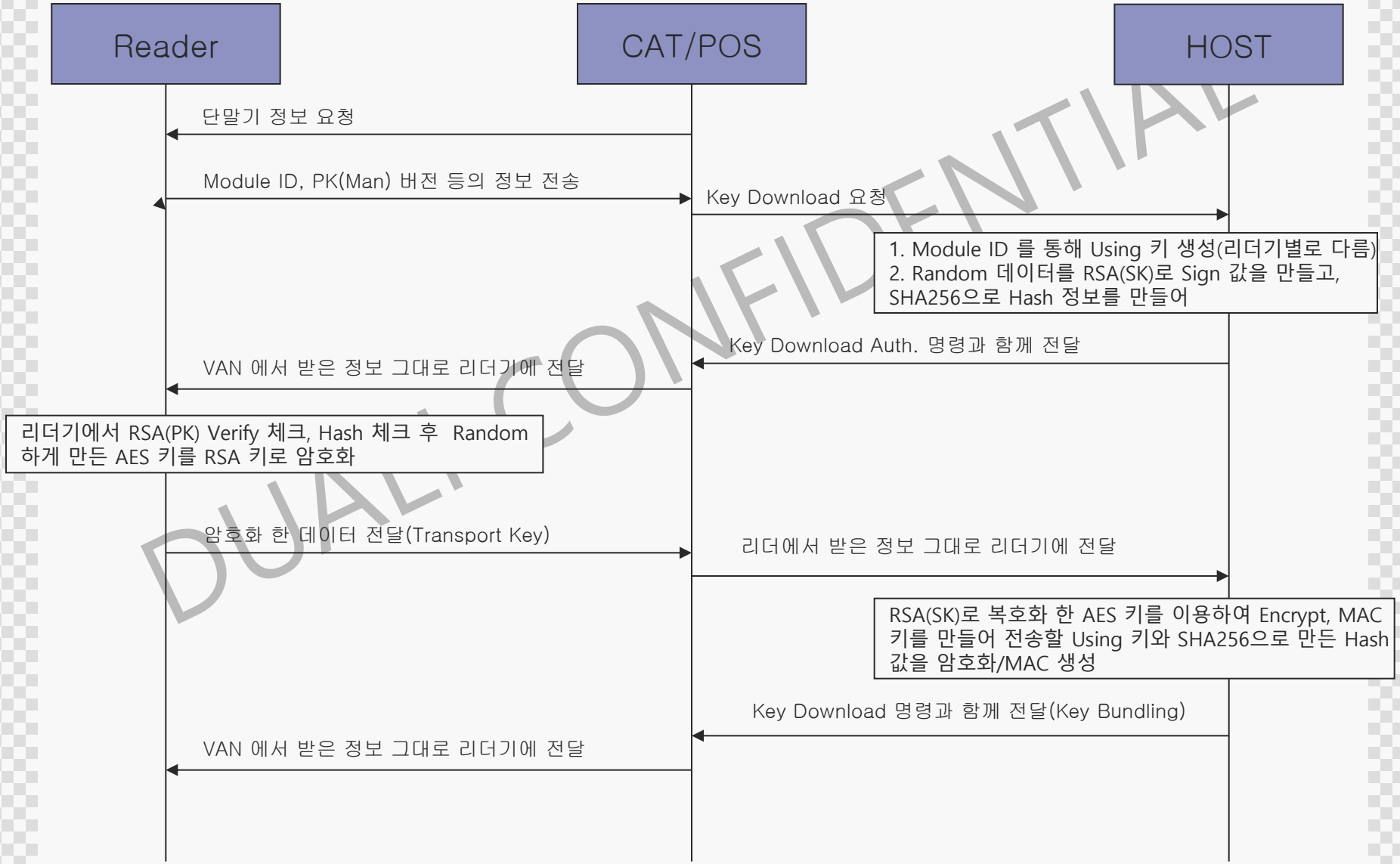
A Technical Report prepared by:
Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Registered with American National Standards Institute

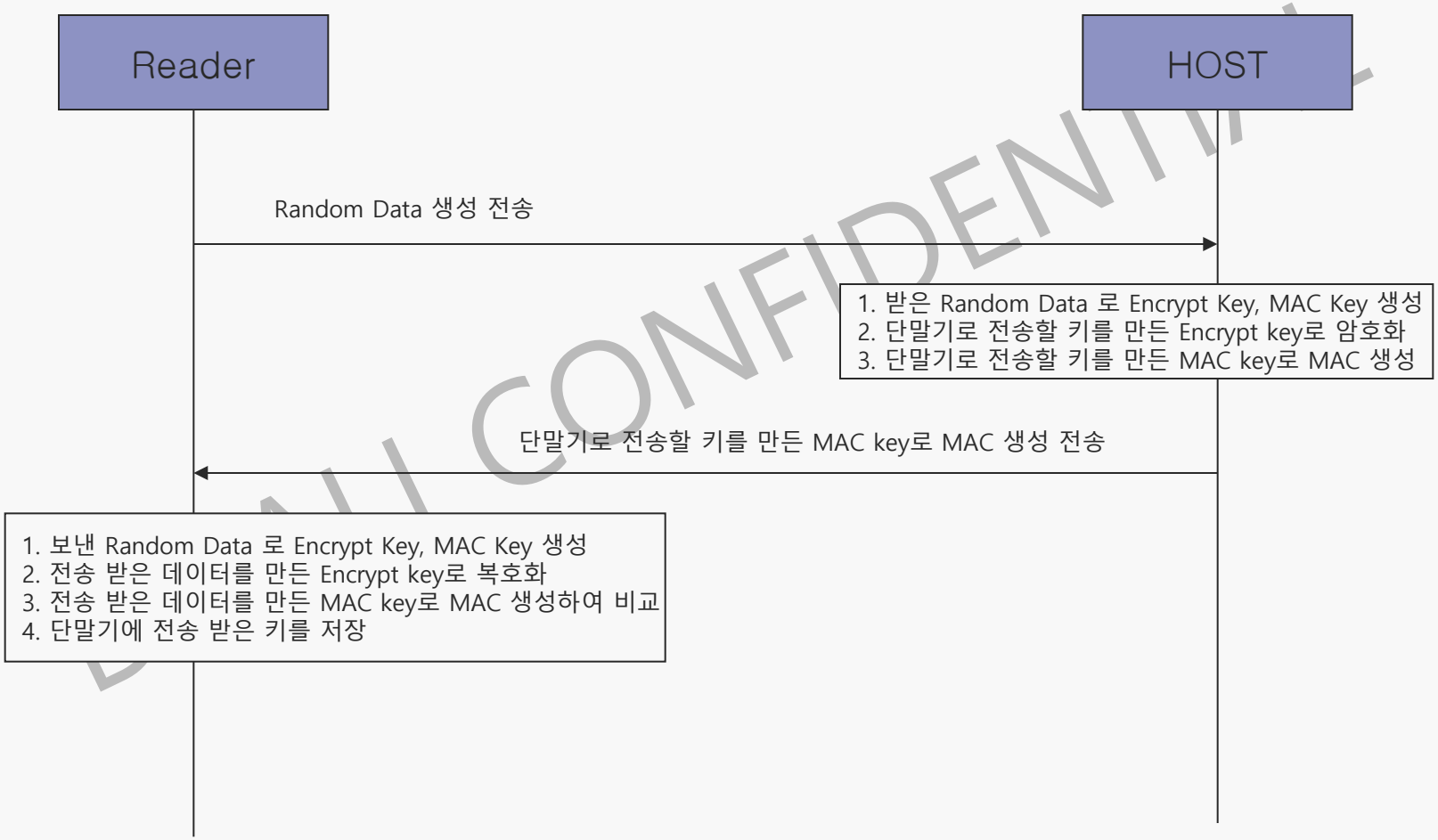
Date Registered: December 9, 2010

Transport Key를 이용하여,
상호 인증을 하기 위한 Bundling
참고 알고리즘(X9 TR-31)

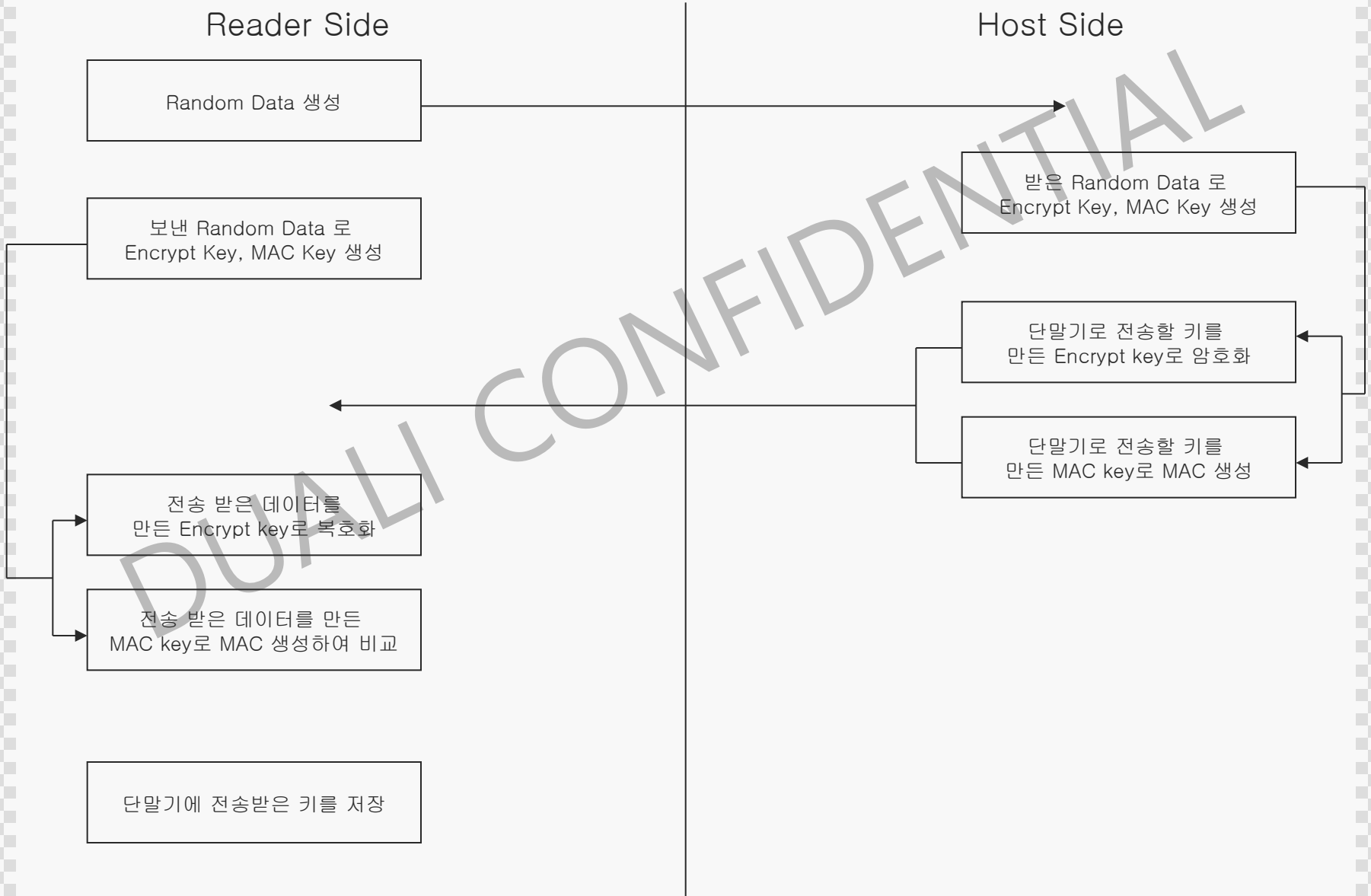
Key Download를 위한 상호 인증



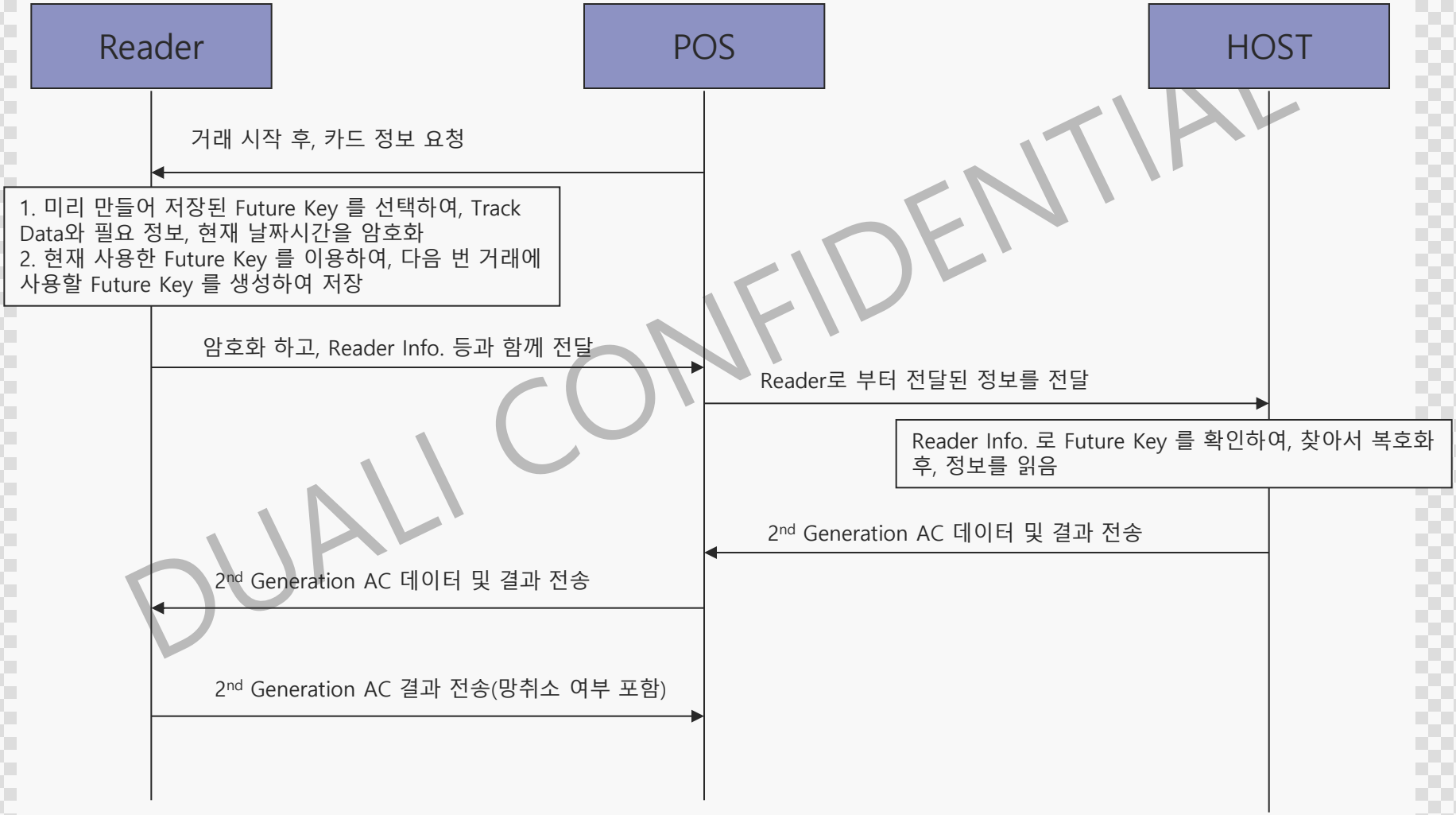
IPEK+KSN Download(1)



IPEK+KSN Download(2)



Data Encrypt(1)



POS 에서는 마스킹 된 카드번호 데이터만 확인 가능
암호화 된 정보와 함께 Reader Info.(REG + Module ID)를 전달

Data Encrypt(2)