PKI 관련 스마트카드 기술규격

2001. 11.

한국정보보호진흥원
전자서명인증관리센터

1. 기술규격명

PKI 관련 스마트카드 기술규격

2. 기술규격의 개요

2.1 목적

스마트카드간 PKI 관련 호환성을 제공하기 위해 관련 기술규격을 정의한다.

2.2 적용범위 및 기대효과

본 기술규격은 전자서명이나 키 분배 관련 응용을 사용하는 스마트카드간의 호환성을 제공하기 위한 파일 구성도 및 메모리 맵을 정의하고 있으며 API, 인증서 및 키의 저장 방법에 관한 요구사항들을 명시하고 있다.

본 기술규격은 스마트카드 내의 PKI 관련 부분을 통합 함으로써 PKI 관련 응용 서비스 활성화에 기여할 것이며 나아가 스마트카드 시장의 활성화에도 기여할 것이다.

본 기술규격은 전자서명인증관리체계내에서 사용되는 전자서명 생성키 및 키분배용 개인키와 인증서를 스마트카드내에 저장하는 기술규격으로 사용될 것이다.

2.3 내용 요약

본 기술규격의 주요내용은 스마트카드 내에서 PKI 관련 응용을 사용할 때 스마트카드간의 호환을 위해 필요한 요구사항에 대한 내용을 기술하고 있다.

3. 관련 표준

3.1 국외 표준 및 규격

ISO 7816 - Contact IC Card 표준
- ISO 7816-1 Physical Characteristics
- ISO 7816-2 Dimensions and location of the contacts

- ISO/IEC 7816-3 Electronic signals and transmission Protocols
- ISO/IEC 7816-4 Inter-industry commands for interchange
- ISO/IEC 7816-5 Numbering system and registration procedure for application identifiers
- ISO/IEC 7816-6 Inter-industry data elements
- ISO/IEC 7816-7 Interindustry commands for Structured Card Query Language (SCQL)
- ISO/IEC 7816-8 Security related interindustry commands

ISO/IEC 10536 - CICC (Contactless IC Card) 표준
- ISO/IEC 10536-1 Physical Characteristics
- ISO/IEC 10536-2 Dimensions and Location of Coupling Areas
- ISO/IEC 10536-3 Electronic signals and mode switching

ISO/IEC 14443 - RCCC (Remote Coupling Communication Card) 표준
- ISO/IEC 14443-1 Physical characteristics
- ISO/IEC 14443-2 Radio frequency interface
- ISO/IEC 14443-3 Transmission Protocols
- ISO/IEC 14443-4 Transmission security features

EMV- IC Card Specification for Payment System
- Part 1 - Electromechanical Characteristics, Logical Interface, and Transmission Protocol
- Part 2 - Data Elements and Commands
- Part 3 - Application Selection
- Part 4 - Security Aspects

EMV- IC Card Terminal Specification for Payment System
- Part 1 - General Requirements
- Part 2 - Software Architecture
- Part 3 - Cardholder, Attendant, and Acquirer Interface

EMV- IC Card Application Specification for Payment System

PC/SC - Interoperability Specification for ICCs and PCs
- Part 1 - Introduction and Architecture Overview
- Part 2 - Interface Requirements for Compatible IC Cards and Readers
- Part 3 - Requirements for PC-Connected Interface Device
- Part 4 - IFD Design Consideration and Reference Design Information
- Part 5 - ICC Resource Manager Definition
- Part 6 - ICC Service Provider Interface Definition

- Part 7 - Application Domain/Developer Design Considerations
- Part 8 - Recommendations for ICC Security and Privacy Devices

목 차

PKI 관련 스마트카드 기술규격

1. 개요

본 기술규격에서는 PKI 관련 정보를 사용하는 모든 스마트카드간의 호환성을 제공하기 위해 기존 공인인증기관 스마트카드에 사용되는 PKI 관련 맵을 기반으로 하여 PKI 관련 스마트카드 기술규격을 규정한다.

2. 구성 및 범위

본 기술규격은 PKI 관련 정보를 사용하는 스마트카드간의 호환성을 제공하기 위한 파일 구성, 메모리 맵, API, 인증서 및 키의 저장 방법에 관한 요구사항들을 명시하고 있다.

또한 암호화를 필요로 하는 어플리케이션 사용 시 키분배용 인증서를 위한 별도의 DF(키분배용 DF)를 사용하며, 스마트카드간 호환성을 보장하기 위해 FID와 WEF 크기 및 API를 통일한다.

본 기술규격은 전자서명인증관리체계내에서 사용되는 전자서명생성키 및 키분배용개인키와 인증서를 저장하는 기술규격으로 사용될 것이다.

3. 관련 표준

3.1 국외 표준 및 규격

가. ISO/IEC 표준

현재 스마트 카드 표준의 근간을 이루는 표준으로서, 폭 넓은 분야에 걸쳐 표준화 작업을 수행하고 있다.

ISO 7816 - Contact IC Card 표준
- ISO 7816-1 Physical Characteristics
- ISO 7816-2 Dimensions and location of the contacts
- ISO/IEC 7816-3 Electronic signals and transmission protocols
- ISO/IEC 7816-4 Inter-industry commands for interchange
- ISO/IEC 7816-5 Numbering system and registration procedure

for application identifiers
- ISO/IEC 7816-6 Inter-industry data elements
- ISO/IEC 7816-7 Interindustry commands for Structured Card Query Language (SCQL)
- ISO/IEC 7816-8 Security related interindustry commands

ISO/IEC 10536 - CICC (Contactless IC Card) 표준
- ISO/IEC 10536-1 Physical Characteristics
- ISO/IEC 10536-2 Dimensions and Location of Coupling Areas
- ISO/IEC 10536-3 Electronic signals and mode switching

ISO/IEC 14443 – RCCC (Remote Coupling Communication Card) 표준
- ISO/IEC 14443-1 Physical characteristics
- ISO/IEC 14443-2 Radio frequency interface
- ISO/IEC 14443-3 Transmission Protocols
- ISO/IEC 14443-4 Transmission security features

나. EMV (Europay MasterCard Visa) 규격

Europay, MasterCard, Visa사 등에서 추진한 금융권 스마트카드규격으로, 다양한 금융서비스를 위한 기술규격사항을 기술하였고, 현재 이 규격에 준하여 대부분의 스마트카드형 신용카드 및 직불카드가 발행되고 있다.

IC Card Specification for Payment System
- Part 1 - Electromechanical Characteristics, Logical Interface, and Transmission Protocol
- Part 2 - Data Elements and Commands
- Part 3 - Application Selection
- Part 4 - Security Aspects

IC Card Terminal Specification for Payment System
- Part 1 - General Requirements
- Part 2 - Software Architecture
- Part 3 - Cardholder, Attendant, and Acquirer Interface

IC Card Application Specification for Payment System

다. PC/SC (Personal Computer/Smart Card) 규격

Microsoft사를 주축으로 여러 업체들이 Workgroup을 결성하여 PC와 IC Card사이의 상호운용을 위한 규격을 제정하였고, 이 규격을 통해 제조회사가 서로 다른 스마트카드와 단말기의 상호운용이 가능하게 되었다.

PC/SC - Interoperability Specification for ICCs and PCs
- Part 1 - Introduction and Architecture Overview
- Part 2 - Interface Requirements for Compatible IC Cards and Readers
- Part 3 - Requirements for PC-Connected Interface Device
- Part 4 - IFD Design Consideration and Reference Design Information
- Part 5 - ICC Resource Manager Definition
- Part 6 - ICC Service Provider Interface Definition
- Part 7 - Application Domain/Developer Design Considerations
- Part 8 - Recommendations for ICC Security and Privacy Devices

4. 약어

본 기술규격에서는 다음의 약어들이 적용된다.

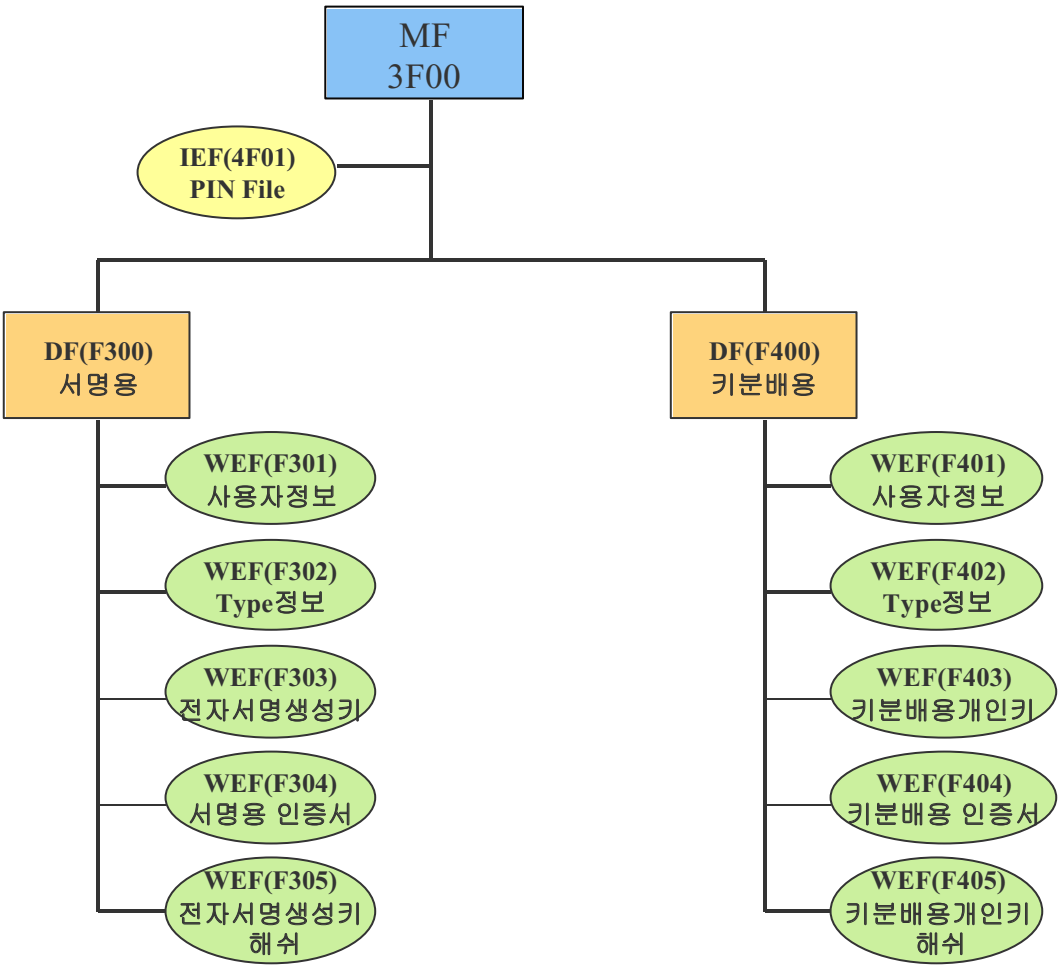
가) MF : Master File
나) DF : Dedicated File
다) EF : Elementary File
라) IEF : Internal Elementary File
마) WEF : Working Elementary File
바) FID : File ID
사) API : Application Program Interface
아) EMV : Europay Master Visa
자) PC/SC : Personal Computer / Smart Card
차) PKI : Public Key Infrastructure

5. PKI 관련 스마트카드 규격

스마트카드내의 PKI 관련 응용에 대한 상호연동을 위해 전자서명인증관리센터에서 지원하는 스마트카드의 규격은 다음과 같다.

5.1 스마트카드 구조

가. 파일 구성도



※ 사용자정보 : 사용자 관련 정보를 기록하기 위해서 사용되는 영역
※ Type 정보 : 사용자카드의 구별자 정보
※ 전자서명생성키 : 사용자의 전자서명생성키 정보를 기록하기 위해 사용되는 영역
※ 서명용인증서 : 사용자의 서명용인증서 정보를 기록하기 위해 사용되는 영역
※ 전자서명생성키해쉬 : 전자서명생성키의 무결성을 점검하기 위한 해쉬값을 기록하기 위해 사용되는 영역
※ 키분배용개인키 : 사용자의 키분배용개인키 정보를 기록하기 위해 사용되는 영역
※ 키분배용인증서 : 사용자의 키분배용인증서 정보를 기록하기 위해 사용되는 영역
※ 키분배용개인키해쉬 : 키분배용개인키의 무결성을 점검하기 위한 해쉬값을 기록하기 위해 사용되는 영역

나. 메모리 MAP

종류		FileID	Size
MF(3F00)	Password 파일	4F01	8 Byte
DF(F300)	사용자 정보	F301	52 Byte
	TYPE 정보	F302	12 Byte
	전자서명생성키	F303	728 Byte
	서명용인증서	F304	1456 Byte
	전자서명생성키 해쉬값	F305	42 Byte
DF(F400)	사용자 정보	F401	52 Byte
	TYPE 정보	F402	12 Byte
	키분배용개인키	F403	728 Byte
	키분배용인증서	F404	1456 Byte
	키분배용개인키 해쉬값	F405	42 Byte

※ 키분배용 FID는 '**F4**XX' 로 확정.
※ 키분배용 WEF들의 크기는 서명용과 동일하게 확정.
※ 기존 E 맵을 사용하는 공인인증기관을 위해 현재 사용중인 관리 프로그램을 F맵과 E맵 모두를 사용할 수 있는 관리프로그램으로 변경 필요.

5.2 PKI 관련 스마트카드 API

PKI 관련 응용을 사용하는 스마트카드는 상호연동을 위해 사용중인 API를 하나의 API로 통일하여 사용하여야 하며, PKI 관련 스마트카드의 API로는 PC/SC를 사용함.

5.3 키 저장방법

전자서명 생성키 및 키분배용 개인키를 스마트카드내에 PKCS#5로 암호화하여 PKCS#8 형태로 저장한다.

5.4 인증서 저장방법

서명용 인증서 및 키분배용 인증서는 DER 형식이나 PEM 형식으로 저장할 수 있다. 파일 크기나 프로그램 적용 용의성을 고려하여 DER 형식으로 저장하는 것을 권고한다.