PKCS #15: Conformance Profile Specification

RSA Laboratories

August 1, 2000

Table of Contents

1 Introduction

For multiple applications to access the PKCS #15 v1.1 standard it will be necessary to ensure that a mechanism exists to ensure interoperability and compliance for at least some specific subset of the specification. To accomplish this task subsets of the PKCS #15 specification have been defined and are detailed in the form of profiles. The profiles specify which sections of the specification need to be implemented for compliance. These profiles can then be used in the production of conformance testing tools and allow vendors to certify their compliance. The aim of this document is to spell out the profile in sufficient detail to allow conformance tools to be implemented and widely adopted.

1 References and related documents

- RSA Laboratories PKCS #1 v2.0: RSA Cryptography Standard.
- RSA Laboratories PKCS #11 v2.10: Cryptographic Token Interface Standard.
- RSA Laboratories PKCS #12 v1.0 (DRAFT): Personal Information Exchange Syntax Standard.
- RSA Laboratories PKCS #15 v1.1: Cryptographic Token Information Format Standard.
- Sweden Post EID: Profile for a PKCS #15 compliant Token.
- FINEID - S4-1 Implementation Profile: Public Key Infrastructure for Smart Cards.

2 Definitions

ANSI: American National Standards Institute. An American standards body.

Application: The implementation of a well-defined and related set of functions that perform useful work on behalf of the user. It may consist of software and or hardware elements and associated user interfaces.

Application provider: An entity that provides an application.

ASN.1 object: Abstract Syntax Notation object as defined in ISO/IEC 8824. A formal syntax for describing complex data objects.

CHV: CardHolder Verification. Also called the PIN. Typically a 4 to 8 digit number entered by the cardholder to verify that the cardholder is authorized to use the card.

Cryptogram: Result of a cryptographic operation.

Data unit: The smallest set of bits that can be unambiguously referenced. Defined in ISO/IEC 7816-4.

Function: A process accomplished by one or more commands and resultant actions that are used to perform all or part of a transaction.

ICC: Integrated Circuit Card. Another name for a smart card.

ISO: International Organization for Standardization

Password: Data that may be required by the application to be presented to the card by its user before data can be processed.

PIN: Personal Identification Number. See CHV.

Provider: Authority who has or who obtained the rights to create the MF or a DF in the card.

Template: Value field of a constructed data object, defined to give a logical grouping of data objects. Defined in ISO/IEC 7816-6.

Token: In this specification, a portable device capable of storing persistent data.

Tokenholder: Analogous to cardholder.

Uniform Resource Identifiers: a compact string of characters for identifying an abstract or physical resource. Described in RFC 2396.

The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in IETF RFC 2119.

3 Symbols and Abbreviations

AODF	Authentication Object Directory File
BER	Basic Encoding Rules
CA	Certificate Authority
CDF	Certificate Directory File
DER	Distinguished Encoding Rules
DF	Directory File

DODF	Data Object Directory File
EF	Elementary File
MF	Master File
ODF	Object Directory File
OID	Object Identifier
PKCS	Public Key Cryptography Standard
PrKDF	Private Key Directory File
PuKDF	Public Key Directory File
SkDF	Secret Key Directory File
URL	Uniform Resource Locator (a class of uniform resource identifiers)

4 General Overview

This document defines profiles for the PKCS #15 v1.1 specification. These profiles specify the data format, access conditions and assumptions necessary for profile conformance. Profiles will be defined using the format defined below

4.1 Profile Model

Scope: The scope will define the purpose and limitations of the profile.

Directory Structure: Explicitly states the specific directory structure for the profile.

File Access Conditions: Lays out the access rules for the files and directories in the profile.

PKCS #15 Object Requirements: States any specific requirements for each required element of the profile.

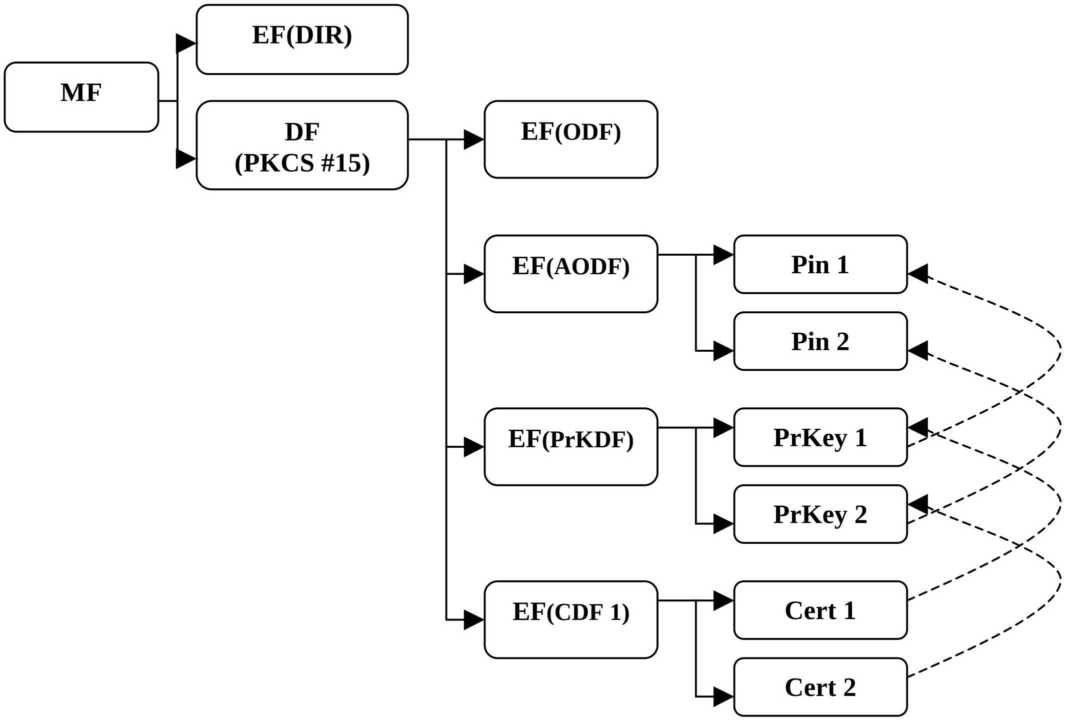
5 Electronic Identification Profile I

5.1 Scope

This section contains a detailed description of an Electronic Identification (EID) profile using a PKCS #15 based token. Two keys are used to control the operations, one key for authentication and encryption, the second for non-repudiation.

5.2 Directory Structure

This sections show the layout for the EFs And DFs for the profile.



5.3 File Access Conditions

This list represents the general access conditions for the EID profile.

File	Access Conditions, R-O card	Access Conditions. R-W card

MF	`Create: SYS`
	`Delete: NEV`
		`Create: SYS`
		`Delete: SYS`

EF(DIR)	`Read:   ALW`
	`Update: SYS`
	`Append: SYS`
		`Read:   ALW`
		`Update: SYS`
		`Append: SYS`

PIN files	`Read:   NEV`
	`Update: NEV`
	`Append: NEV`
		`Read:   NEV`
		`Update: CHV`
		`Append: NEV`

DF(PKCS15)	`Create: SYS`
	`Delete: NEV`
		`Create: CHV | SYS`
		`Delete: SYS`

EF(TokenInfo)	`Read:   ALW`
	`Update: NEV`
	`Append: NEV`
		`Read:   ALW`
		`Update: CHV | SYS | NEV`
		`Append: NEV`

EF(ODF)	`Read:   ALW`
	`Update: NEV`
	`Append: NEV`
		`Read:   ALW`
		`Update: SYS`
		`Append: SYS`

AODFs	`Read:   ALW`
	`Update: NEV`
	`Append: NEV`
		`Read:   ALW`
		`Update: NEV`
		`Append: CHV | SYS`

PrKDFs, PuKDFs	`Read:   ALW | CHV`
	`Update: NEV`
	`Append: SYS | NEV`
		`Read:   ALW | CHV`
		`Update: CHV | SYS | NEV`
		`Append: CHV | SYS`

Key files (see details in section 5.4.1)	`Read:   NEV`
	`Update: NEV`
	`Append: NEV`
	`Crypt:  CHV`
		`Read:   NEV`
		`Update: CHV | SYS | NEV`
		`Append: CHV | SYS | NEV`
		`Crypt:  CHV`

Other EFs in the PKCS15 directory	`Read:   ALW | CHV`
	`Update: NEV`
	`Append: SYS | NEV`
	`Crypt:  CHV` (when applic.)
		`Read:   ALW | CHV`
		`Update: CHV | SYS | NEV`
		`Append: CHV | SYS | NEV`
		`Crypt:  CHV` (when applic.)

.

5.4 PKCS #15 Object Requirements

5.4.1 Private Keys

At least two private keys must be present on the PKCS #15 token. One key is used is used for both authorization and encryption. The second key is used exclusively for non-repudiation (or digital signatures).

The allowed private key type is RSA keys of strength 1024 or greater.

5.4.1.1 Private Key 1 (Authentication and encryption)

PrKey1 must be verified by PIN 1 before private key operations are initially performed. The access conditions for this key is:

EF(PrKey)	`Read:`	`NEV`
	`Update:`	`NEV`
	`PrKey Ops:`	`PIN 1`

5.4.1.2 Private Key 2 (Non-Repudiation)

PrKey2 must be verified by PIN 2 before each private key operation is performed. The user must type the PIN for each operation:

EF(PrKey)	`Read:`	`NEV`
	`Update:`	`NEV`
	`PrKey Ops:`	`PIN 2`

5.4.2 Certificates

For each private key at least one corresponding **X509Certificate** type certificate must be stored in the token and pointed to by the CDF. Host side applications are required to recognize and use the **X509Certificate** type. The access conditions for each of the certificates are:

EF(Cert)	`Read:`	`ALW`
	`Update:`	`PIN 1`

5.4.3 Authentication Objects

At least two authentication objects must exist on the token for protection of private objects. The second authentication object (PIN2) is used only to authenticate non-repudiation objects. PIN2 also has the requirement that the verification status is automatically dropped to “not verified” by the card after each non-repudiation private key operation.

Other PIN conditions are:

PINs must be at least 4 characters long.

BCD, UTF8 or ASCII encoding is used.

After three consecutive failed PIN authorization attempts the PIN is blocked.

Unblocking and disable routines are defined by the application issuer.

A pin can be unblocked any number of times.

The application issuer defines the unblocking procedure.

Pin update is a special operation defined by the application issuer. The usual access conditions for each of the PINs are:

EF(PIN)	`Read:          NEV`
	`Update PIN1:  PIN1`
	`Update PIN2:  PIN2`