

# YD

## 中华人民共和国通信行业标准

YD/T 3202—2016

---

### 移动通信终端访问电信智能卡 安全技术要求

Access control requirements for telecom smartcard

2016-10-22 发布

2017-01-01 实施

---

中华人民共和国工业和信息化部 发布

目 次

前言..... II

1 范围..... 1

2 规范性引用文件..... 1

3 术语、定义和缩略语..... 1

    3.1 术语和定义..... 1

    3.2 缩略语..... 2

4 电信智能卡访问控制概述..... 2

    4.1 简介..... 2

    4.2 系统架构..... 3

5 电信智能卡访问控制规则要求..... 3

    5.1 访问控制规则文件要求..... 3

    5.2 电信智能卡接口要求..... 9

6 移动通信终端访问控制技术要求..... 11

    6.1 概述..... 11

    6.2 应用签名证书获取要求..... 12

    6.3 规则加载要求..... 12

    6.4 规则匹配要求..... 13

附录 A（资料性附录）规则举例..... 18

## 前 言

本标准采用重新起草法参考 GlobalPlatform 标准《安全单元访问控制 V1.0 (Secure Element Access Control V1.0)》编制，与该标准的一致性程度为非等效。其主要技术差异如下：

- GP规范定义了两种访问控制方案，即ARA方案（基于卡应用管理规则的方案）和ARF方案（基于文件管理规则的方案），考虑到电信智能卡本身的特点以及目前方案的成熟程度，本标准使用了ARF方案。

- 针对ARF方案做了重新组织。为了便于卡商和终端厂商分别参考，对标准内容按照电信智能卡 and 智能终端的要求分别进行了编排。

- 由于电信智能卡接口涉及终端与卡的互通，因此本标准在GP规范的基础上增加了5.2节，即电信智能卡接口要求。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国移动通信集团公司。

本标准主要起草人：任晓明、李 琳。

# 移动通信终端访问电信智能卡安全技术要求

## 1 范围

本标准规定了电信智能卡访问控制方案，包括电信智能卡、移动通信终端的功能及接口要求等内容。

本标准适用于移动通信终端和电信智能卡（不包括嵌入式 SE、嵌入式 UICC 卡）。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- |                 |   |
|-----------------|---|
| ITU-T X.690     | 信息技术-抽象语法符号1 编码规则规范：基本编码规则、典型编码规则 and 高级编码规则（Information technology – ASN.1 encoding rules:Specification of Basic Encoding Rules (BER),Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)） |
| ETSI TS 102.221 | 智能卡：UICC-终端接口；物理和逻辑特性（Smart Cards;UICC-Terminal interface;Physical and logical characteristics）   |
| RSA Lab PKCS#15 | 加密令牌信息语法标准（Cryptographic Token Information Syntax Standard）   |

## 3 术语、定义和缩略语

### 3.1 术语和定义

下列术语和定义适用于本文件。

#### 3.1.1

**电信智能卡 Telecom Smartcard**

支持电信功能的智能卡，包括SIM卡、USIM、CSIM卡等。

#### 3.1.2

**访问控制模块 Access Control Enforcer**

作为电信智能卡访问 API 的一部分，从电信智能卡内获取访问控制规则并根据这些规则对终端应用访问电信智能卡应用的操作进行控制。



3.1.3

**终端应用 Device Application**

运行在终端操作系统内的第三方应用程序。

3.1.4

**移动通信终端 Mobile Device**

具有移动通信功能的终端设备。

3.1.5

**电信智能卡应用 Telecom Smartcard Application**

安装并运行在电信智能卡内的软件应用。

3.1.6

**终端应用SE编程接口 SE-API**

为终端应用提供的访问电信智能卡的编程接口。

3.2 缩略语

下列缩略语适用于本文件。

ACCF	Access Control Conditions File	访问控制条件文件
ACMF	Access Control Main File	访问控制主文件
ACRF	Access Control Rules File	访问控制规范文件
AID	Application IDentifier, following ISO/IEC	应用标识
APDU	Application Protocol Data Unit	应用协议数据单元
API	Application Programming Interface	应用编程接口
ASN.1	Abstract Syntax Notation One	抽象语法符号
DF	Dedicated File	专用文件
DODF	Data Object Directory File	数据对象目录文件
EF DIR	Elementary File Directory	单元文件目录
NFC	Near Field Communication	近场通信
ODF	Object Directory File	对象目录文件
PKCS#15	Public-Key Cryptography Standards #15	公钥密码学标准#15, 本标准中以此缩写代表标准中定义的文件系统格式

4 电信智能卡访问控制概述

4.1 简介

本标准中定义了一种电信智能卡访问控制机制, 这种访问控制的目标是阻止对电信智能卡中资源

的非授权访问，同时可以防止针对电信智能卡的拒绝服务攻击。

终端操作系统实现访问控制的依据是存储在电信智能卡中的访问控制规则。这些规则定义了哪个（或哪些）终端应用可以访问哪个（或哪些）电信智能卡应用，也可以定义允许访问的具体指令。

## 4.2 系统架构

电信智能卡访问控制系统架构如图 1 所示。

该架构定义了一个电信智能卡访问控制的通用机制，即由发卡方统一管理访问控制规则，并将规则写入电信智能卡中的 PKCS#15 规则文件，移动通信终端的访问控制模块通过文件接口读取规则，并在终端应用通过 SE-API 访问电信智能卡过程中，根据规则判断是否允许访问。

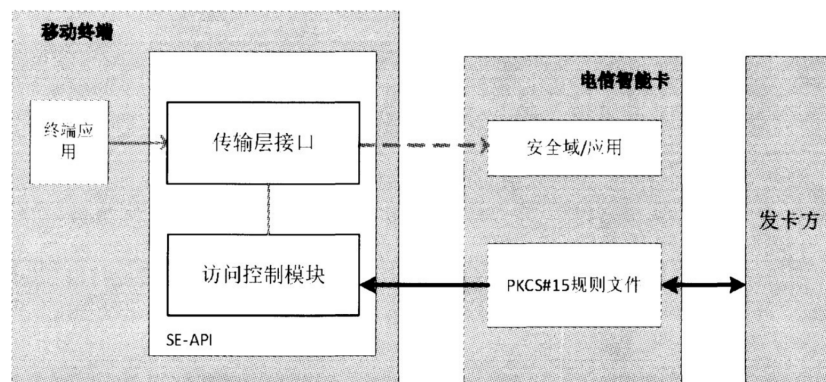


图 1 电信智能卡访问控制系统架构

## 5 电信智能卡访问控制规则要求

### 5.1 访问控制规则文件要求

#### 5.1.1 概述

访问控制规则文件存储在电信智能卡中的 PKCS#15 文件结构内，其中包含 ODF、DODF、ACMF、ACRF、ACCF 等 EF 文件，下面将介绍相应的文件系统结构定义，对于 ASN.1 的对象定义，如非显式说明（如 AID），则基于 ASN.1 编码规则进行描述（见 ITU-T X.690）。附录 A 中给出了规则文件的举例。

#### 5.1.2 文件填充

访问控制规则文件末尾仅可使用 0xFF 进行填充。访问控制机制中用于管理文件的文件解析引擎应支持这种填充方式。

#### 5.1.3 EF DIR 文件

本标准中，如果采用 DF 组织规则文件，则需要采用 EF DIR 文件中配置 PKCS#15 DF 入口，其中包括 PKCS#15 应用的 AID 及 DF 路径信息。

EF DIR 的总体格式要求见 ETSI TS 102.221 的定义，对于 PKCS#15 入口的定义要求见 RSA Lab

PKCS#15。

5.1.4 ODF 文件

ODF 存储了 DODF 文件的路径，该文件的结构定义见表 1。

表 1 ODF 文件定义

文件标识: '5031'		文件类型: transparent file		M/O: Mandatory	
文件长度: $n$ 字节			更新频率: low		
存取条件:					
READ		ALW			
UPDATE		ADM			
DEACTIVATE		ADM			
ACTIVATE		ADM			
Bytes No.	描述		M/O	Length/byte	
1~ $n$	DODF文件的路径 (ASN.1格式)		M	$n$ 字节	

ODF 文件的 ASN.1 格式定义如下:

```
Path ::= SEQUENCE {  
    path OCTET STRING,  
    index INTEGER (0..pkcs15-ub-index) OPTIONAL,  
    length [0] INTEGER (0..pkcs15-ub-index) OPTIONAL  
}( WITH COMPONENTS {..., index PRESENT, length PRESENT}|  
   WITH COMPONENTS {..., index ABSENT, length ABSENT})
```

5.1.5 DODF 文件

DODF 文件存储了 GP 访问控制应用的标识以及 ACMF 文件的路径。该文件的结构定义见表 2。

表 2 DODF 文件定义

文件标识: 'XXXX'		文件类型: transparent file		M/O: Mandatory	
文件长度: $n$ 字节			更新频率: low		
存取条件:					
READ		ALW			
UPDATE		ADM			
DEACTIVATE		ADM			
ACTIVATE		ADM			
Bytes No.	描述		M/O	Length/byte	
1~ $n$	包含Oid及ACMF的Path等信息（ASN.1格式）		M	$n$	

访问控制数据读写的入口为 PKCS#15 DODF, 该入口采用访问控制OidDO( {iso(1) member-body(2) country-USA(840) Global-Platform(114283)} )。

访问控制机制 OID 为： {iso(1) member-body(2) country-USA(840) Global-Platform(114283) device(200) seAccessControl(1) accessControlMainFile(1)}。

DODF OidDO 对象包含 ACMF 文件的路径。该路径的 ASN.1 格式定义如下：

```
Path ::= SEQUENCE {
    path OCTET STRING,
    index INTEGER (0..65535) OPTIONAL,
    length [0] INTEGER (0..65535) OPTIONAL
} ( WITH COMPONENTS { ..., index PRESENT, length PRESENT } |
    WITH COMPONENTS { ..., index ABSENT, length ABSENT } )
-- the path of a file (as per PKCS#15)
```

5.1.6 ACMF 文件

ACMF，即访问控制主文件，每个电信智能卡中应只存在一个 ACMF 文件。如果电信智能卡中出现多个 ACMF 文件，应视为该电信智能卡受到了攻击，访问控制模块（Access Control Enforcer）应禁止一切对相应的电信智能卡中应用的访问。

ACMF 文件中包含了刷新标记（refresh tag）和访问控制规则的路径。ACMF 文件的结构见表 3。

表 3 访问控制主文件定义（ACMF）

文件标识: 'XXXX'		文件类型: transparent file		M/O: Mandatory	
文件长度: $n$ 字节			更新频率: low		
存取条件:					
READ		ALW			
UPDATE		ADM			
DEACTIVATE		ADM			
ACTIVATE		ADM			
Bytes No.	描述		M/O	Length/byte	
1~ $n$	文件内容包含刷新标记（Refresh Tag）和访问控制规则文件路径，采用ASN.1格式定义		M	$n$ 字节	

ACMF 对象采用如下 ASN.1 语法进行定义：

```
-- The access control main file object
AccessControlMainFile ::= SEQUENCE {
    -- the refresh tag
    refreshTag OCTET STRING (SIZE(8)),
    -- the path to the access control rules file
    rulesFile Path,
```

-- RFU

...

}

### 5.1.7 ACRF 文件

ACRF，即访问控制规则文件。每个电信智能卡中应只存在一个 ACRF 文件。如果电信智能卡中出现多个 ACRF 文件，应视为电信智能卡受到了攻击，访问控制模块（Access Control enforcer）应禁止一切对相应的电信智能卡中应用的访问。

ACRF 文件中每条规则显式或隐式定义了一组电信智能卡应用的标识，并指向用于定义如何访问这些应用的访问控制条件文件（ACCF）。

ACRF 采用表 4 给出的结构定义。

表 4 访问控制主文件定义（ACRF）

文件标识: 'XXXX'		文件类型 transparent file		M/O: Mandatory	
文件长度: $n$ 字节			更新频率: low		
存取条件:					
READ		ALW			
UPDATE		ADM			
DEACTIVATE		ADM			
ACTIVATE		ADM			
Bytes No.	描述		M/O	Length/byte	
1 ~ $n$	访问控制规则列表，每个表项包含：目标+访问控制条件 文件路径。规则列表采用ASN.1格式定义，见后续说明		M	$n$ 字节	

访问控制规则采用如下 ASN.1 语法定义：

-- An access control rule entry

Rule ::= SEQUENCE {

-- the target of this policy entry,

target Target,

-- the path to the access control conditions file applicable

-- for this target

conditionsFile Path,

-- RFU

...

}

目标对象指明了规则的适用范围：某个电信智能卡应用（通过 AID 指定）、默认选择的应用或所有其他应用（没有被一条特定规则显式保护的所有的电信智能卡应用）。

目标对象采用如下 ASN.1 语法定义：

-- An access control target: either a named application,  
-- the default selected application, or all other applications

Target ::= CHOICE {  
    -- the AID of the targeted Secure Element application  
    aid [0]EXPLICIT AID,  
    -- the (unnamed) default selected Secure Element  
    -- application (applies to default selected application  
    -- on all logical channels)  
    default [1]NULL,  
    -- identifies all other applications  
    -- that are not referenced in another rule  
    others [2]NULL,  
    -- RFU  
    ...  
}

AID 对象采用如下 ASN.1 语法定义:

-- as per ISO7816-5  
AID ::= OCTET STRING

5.1.8 ACCF 文件

访问控制规则引用的条件存储于 ACCF 文件，即访问控制条件文件中。所有访问控制条件采用列表的形式，列表中每条记录包含了一个被授权的应用发布者证书的 SHA1 算法哈希值。

如果访问控制条件文件为空，则指向这个文件的访问控制规则会拒绝所有终端应用对该规则对象所指向的电信智能卡应用的访问。

如果访问控制条件文件中未指定证书哈希值，则所有指向这个条件文件的访问控制规则会允许所有终端应用对该规则指向的电信智能卡应用的访问。

ACCF 采用表 5 给出的结构定义。

表 5 确访问控制条件文件定义（ACCF）

文件标识：‘XXXX’	文件类型：transparent file	M/O: Mandatory
文件长度：n字节	更新频率：low	
存取条件：		
READ	ALW	
UPDATE	ADM	
DEACTIVATE	ADM	
ACTIVATE	ADM	

表 5 确访问控制条件文件定义 (ACCF) (续)

Bytes No.	描述	M/O	Length/byte
1~ <i>n</i>	访问控制条件包括如下内容： 1. 证书的哈希值 (M) 2. 访问控制规则： ◇ APDU许可策略 (O) ◇ NFC许可策略 (O) 以上内容采用ASN.1格式定义，见后续说明	M	<i>n</i> 字节

访问控制条件采用如下 ASN.1 语法定义：

-- A Condition entry

Condition ::= SEQUENCE {

-- the hash of the certificate of the authorized entity;  
-- if not indicated, then the Rule pointing to this Condition  
-- applies to all the device applications  
cert CertHash OPTIONAL,  
accessRules [0]AccessRules OPTIONAL,  
-- RFU  
...

}

-- SHA1 of the certificate of the authority being granted access

CertHash ::= OCTET STRING (SIZE(20))

-- Each type of AccessRule can occur not more than once

-- in this sequence

AccessRules ::= SEQUENCE OF AccessRule

AccessRule ::= CHOICE {

apduAccessRule [0]APDUAccessRule,  
nfcAccessRule [1]NFCAccessRule

}

APDUAccessRule ::= CHOICE {

apduPermission [0] APDUPermission,  
apduFilter [1] APDUFilters  
-- RFU

...

}

```

-- TRUE means APDU access is allowed,
-- FALSE means APDU access is not allowed
APDUPermission ::= BOOLEAN

-- Each APDU filter is a 8 byte octet string:
-- 4-byte header and 4-byte mask
APDUFilters ::= SEQUENCE OF APDUFilter
APDUFilter ::= OCTET STRING (SIZE(8))
NFCAccessRule ::= CHOICE {
    nfcPermission [0] NFCPermission,
    -- RFU
    ...
}
-- TRUE means NFC event is allowed,
-- FALSE means NFC event is not allowed
NFCPermission ::= BOOLEAN

```

由于 APDU 许可或 NFC 事件策略是可选项，所以相应的访问控制规则可能未在规则文件中定义。如果未定义，终端访问控制模块采用如下方式处理：

- 对于一个特定 AID 或其他 AID，如果 ARF 中未定义相关 APDU 策略时，则终端访问控制模块将缺失的 APDU 许可策略解释为 ALWAYS 允许策略。
- 对于一个特定 AID 或其他 AID，如果 ARF 中未定义相关 NFC 事件策略时，则终端访问控制模块将缺失的 NFC 事件策略解释为 ALWAYS 允许策略。

## 5.2 电信智能卡接口要求

### 5.2.1 概述

电信智能卡需要提供如下 APDU 指令接口，用于规则的加载（该接口在 ETSI TS 102.221 规范中 APDU 定义的基础上进行了简化）。对于规则更新的机制，不在本标准的范围。

### 5.2.2 SELECT

#### 5.2.2.1 指令说明

SELECT 命令用于选择一个应用或文件，卡支持利用 SELECT 命令打开一个逻辑信道或选择规则文件。

#### 5.2.2.2 指令参数和数据

SELECT 命令报文含义见表 6。



表 6 SELECT 命令报文

编码	值	含义
CLA	0X	
INS	'A4'	SELECT
P1	'xx'	引用控制参数P1
P2	'xx'	引用控制参数P2
Lc	'xx'	AID或文件路径长度
Data	'xxxx...'	选择应用的AID或文件路径
Le	'00'	

SELECT引用控制参数P1见表7。

表 7 SELECT 引用控制参数 P1

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	0	根据文件路径进行选择
0	0	0	0	0	1	0	0	根据名称进行选择

SELECT引用控制参数P2见表8。

表 8 SELECT 引用控制参数 P2

b8	b7	b6	b5	b4	b3	b2	b1	含义
						0	0	第一个或仅一个
						1	0	下一个匹配项

### 5.2.2.3 响应报文

SELECT响应报文数据域由被选择应用或文件的特定信息组成。

成功执行完该命令后，返回状态字'9000'，指令执行失败包括如表9所示错误状态。

表 9 SELECT 错误状态

SW1	SW2	说明
'6A'	'81'	不支该功能
'6A'	'82'	没有发现选择的应用/文件

### 5.2.3 READ BINARY

#### 5.2.3.1 指令说明

该指令从当前 EF 文件中读取字节流，只有在该 EF 文件满足读权限时才可以执行。

#### 5.2.3.2 指令参数和数据

READ BINARY指令参数见表10。

表 10 指令参数

代码	值	含义
CLA	0X	
INS	B0	
P1	'xx'	见表5.11
P2	'xx'	偏移量低字节
Lc	'xx'	空
Data	'xxxx...'	空
Le	X	待读取字节数

READ BINARY 指令 P1 编码见表 11。

表 11 P1 编码

b8	B7	b6	b5	b4	b3	b2	b1	说明
0	X	X	X	X	X	X	X	b7~b1是待读取数据的偏移量，P2是偏移量的低字节

READ BINARY 指令响应数据见表 12。

表 12 响应数据

字节	说明	长度
1 ~ Le	读取的数据	Le

5.2.3.3 响应状态值

READ BINARY指令响应状态值见表13。

表 13 响应状态

SW1	SW2	说明
'90'	'00'	正常返回
'6A'	'80'	参数错误
'69'	'85'	使用条件不满足

6 移动通信终端访问控制技术要求

6.1 概述

移动通信终端的访问控制模块是完成访问控制功能的核心模块，该模块应提供规则匹配的核心功能，并实现证书获取、规则管理、规则匹配等功能。

需要强调的是，移动通信终端中访问控制模块是终端应用访问电信智能卡的必经渠道，也就是说终端设计上必须确保访问控制模块所提供的访问控制策略不可绕过。

## 6.2 应用签名证书获取要求

访问控制模块可以通过终端操作系统提供的 API 获取已经安装应用的证书或证书链信息。如果终端应用有多个签名，访问控制模块会获取每个签名相关的证书。访问控制模块会计算出每个证书的哈希值。如果终端应用是由一个证书链签发，则需要获取证书链中的每一级证书的哈希值。

## 6.3 规则加载要求

### 6.3.1 概述

在规则加载过程中，终端访问控制模块需要符合规则文件的兼容性处理要求，同时，在规则读取前需要对卡片中规则文件结构的合法性进行验证。

### 6.3.2 规则文件选择要求

规则文件在电信智能卡内的存储结构有不同的实现方式，访问控制模块应该能够做兼容性处理，以支持不同的卡片实现。

PKCS#15 文件的选择要求如下：

第一步：终端以 PKCS#15 AID (A0 00 00 00 63 50 4B 43 53 2D 31 35) 作为参数发送 SELECT\_BY\_NAME 命令给卡片，如果选择成功，则终端可以开始读取 PKCS#15 文件 (ODF、DODF 等)；

第二步：如果第一步中的选择失败，则按以下步骤处理：

a) 终端发送 SELECT 指令选择 MF 和 EF DIR；

b) 终端读取 EF DIR 并查找与 PKCS#15 AID (A0 00 00 00 63 50 4B 43 53 2D 31 35) 相匹配的入口 (DF-PKCS#15)；

c) 如果 PKCS#15 入口查找成功，终端选择 PKCS#15 DF 目录，然后可开始依次读取 ODF, DODF 等文件。

### 6.3.3 访问控制规则文件系统合法性验证

如果文件系统满足以下条件时，则认为规则文件系统正确定义：

- 卡片上存在 PKCS#15 应用（通过 AID 可以选择成功），访问控制机制的 OID 在 DODF 文件中正确配置；

- PKCS#15 文件结构在 EF dir 中引用，并且访问控制机制的 OID 在 DODF 文件中正确配置。

如果规则文件系统满足以下条件中的任一条时，则认为规则文件系统中没有访问控制规则，其他的异常情况将认为是文件解析错误。

- 没有 PKCS#15 应用（不能通过标准 AID 选择成功），并且没有 EFdir 文件；

- 没有 PKCS#15 应用（不能通过标准 AID 选择成功），并且 EFDir 文件中没有指定 PKCS#15 文件结构入口；

- PKCS#15 文件结构存在于电信智能卡中，但访问控制机制的 OID 在 DODF 文件中未指定。

没有访问控制规则以及文件解析错误，均导致拒绝任何终端应用访问电信智能卡。

### 6.3.4 规则加载流程

访问控制模块使用的规则需要从电信智能卡中读取、解析并缓存在终端，规则加载的时机如下：

- 终端初始化过程；
- 规则匹配过程中发现规则更新。

相应的规则加载流程如图 2 所示。

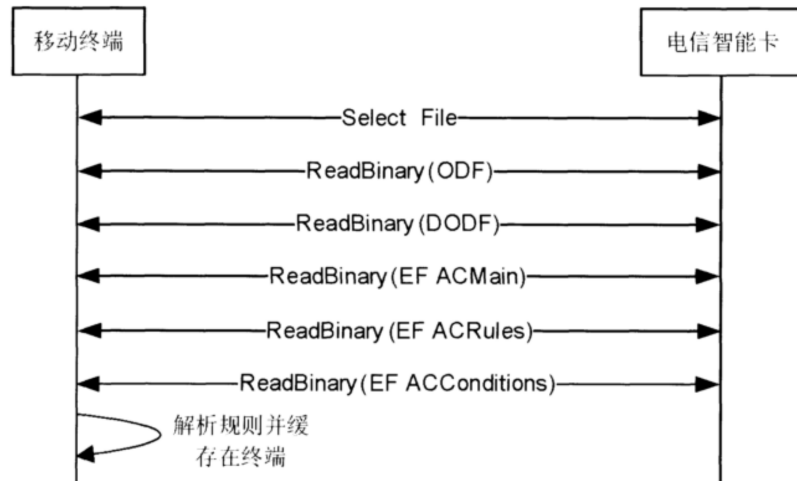


图 2 规则加载流程

流程说明：

1. 移动通信终端选择电信智能卡的规则文件；
2. 读取 ODF 获取 DODF 文件路径；
3. 读取 DODF 获取 ACMain 文件路径；
4. 读取 ACMain 文件获取 ACRules 文件路径；
5. 读取 ACRules 获取 ACConditions 文件列表；
6. 移动通信终端访问控制模块解析规则文件并将规则信息缓存到终端。规则读取后需要按照规则的格式进行解析，如果发现规则解析错误，则终止解析过程，电信智能卡禁止任何终端应用访问。在规则解析完毕后，将解析后的规则缓存在终端内存（终端关机后清除缓存）。

## 6.4 规则匹配要求

### 6.4.1 概述

规则匹配是访问控制模块的核心功能。在访问控制模块接收到终端应用访问电信智能卡应用的请求后，需要根据终端应用的标识、该应用要访问的目标电信智能卡应用以及具体的访问指令等信息在访问控制规则库中找到最佳的匹配规则，并根据规则的要求决定是否对该请求授权。

规则匹配过程中，访问控制模块需要按照规则匹配算法进行匹配，同时访问控制模块需要处理多条规则都能够匹配的情况。

## 6.4.2 规则冲突处理

### 6.4.2.1 概述

由于针对同样的访问控制需求，规则的定义可能严格也可能宽松、可能具体也可能通用、可能限定一个应用也可能限定多个应用，因此，可能会出现不同访问控制规则发生冲突的情况，也就是多条规则都可以匹配相同访问控制请求，那么就需要定义处理规则冲突的方法。

具体来说，规则冲突处理主要有如下两种情况：

- a) 首先是如果多条规则都可以匹配，需要定义优先级机制，并选择优先级最高的规则进行匹配；
- b) 如果多条规则匹配且优先级相同，则需要定义规则聚合处理的机制。

### 6.4.2.2 规则优先级处理

对于规则匹配过程中发现多条规则可以匹配的情况下，规则的匹配不是基于读取的顺序进行，而需要依次按照如下三个基本原则进行优先级处理：

- a) 具体的规则比通用的规则优先级高

具体的规则是指通过如下方式，显示地与某个具体实体相关联：

- 电信智能卡应用：通过指定 AID 或者指定缺省应用的方式与某个电信智能卡应用相关联；
- 终端应用：通过指定签名证书的方式与某个终端应用相关联。

表 14 从高到低列出了规则的具体程度的排序。

表 14 规则优先级

电信智能卡应用是否被显式指定	终端应用是否被显式指定	优先级
是	是	最高
是	否	高
否	是	低
否	否	最低

- b) 证书链中的下级证书优先级更高

如果终端应用是由证书链中的某个证书签名，那么在搜索最具体（优先级最高）的规则时，应优先对签名终端应用的证书（末端实体证书）进行搜索，然后依次搜索证书链中的上级证书，直到找到证书（具有同样级别的具体化）。如果没有找到（也只有在这种情况下），会继续搜索下一优先级的规则。

- c) 严格的规则优先级更高

最严格的规则是禁止终端应用访问电信智能卡；次之是只允许特定 APDU 访问电信智能卡。最不严格的规则是永远允许终端应用访问电信智能卡。

### 6.4.2.3 规则的聚合

如果多条规则适用于同样的电信智能卡应用并具有同样的优先级，那么对这些规则应做聚合处理，并且更加严格的规则比宽松规则具有更高的优先级。如果两条规则有同样严格的数据，那么数据需要进行合并处理，处理方式见表 15。

表 15 访问控制规则冲突处理方案

规则冲突处理方案			R1					
			All			AID		
			Never	Filter	Always	Never	Filter	Always
R2	All	Never	$R1=R2$	$R2$	$R2$	$R1$		
		Filter	$R1$	$R1+R2$	$R2$			
		Always	$R1$	$R1$	$R1=R2$			
	AID	Never	$R2$			$R1=R2$	$R2$	$R2$
		Filter				$R1$	$R1+R2$	$R2$
		Always				$R1$	$R1$	$R1=R2$

如果存在一条指定了终端应用证书哈希值和电信智能卡应用 AID 的具体规则，那么除非有针对其他终端应用的具体规则，否则其他的终端应用访问这个 SE 应用都应被拒绝。

### 6.4.3 规则匹配算法

#### 6.4.3.1 基于单一证书的规则匹配

下面对访问控制模块采用的规则匹配算法进行说明。

首先，在如下情况下访问控制模块应该拒绝终端应用访问电信智能卡的请求：

- 规则文件不存在；
- 规则文件存在，但不存在显示授权终端应用访问的规则；
- 在读取和解析访问控制规则过程中出现错误。

访问控制模块采用下面的算法获取并使用和指定终端应用及电信智能卡应用相关联的访问控制规则，其中终端应用由签名证书标识，电信智能卡应用由 AID 标识。

- 首先，搜索指定了终端应用和电信智能卡应用的具体规则：

**SearchRuleFor(DeviceApplicationCertificate, AID)**

- 如果规则存在，则应用这条规则，停止搜索过程。
- 如果存在另一个终端应用和该电信智能卡应用相关联的具体规则，那么，**SearchRuleFor(DeviceApplicationCertificate, AID)**搜索的结果应该是“Never”（见“规则冲突处理”部分的说明）。

- 如果没有规则满足条件 a)，则需要继续搜索针对所有终端应用（而不是指定具体应用），并且通过 AID 指定了具体的电信智能卡应用的规则：

**SearchRuleFor(<AllDeviceApplications>, AID)**

- 如果存在另一个终端应用和该电信智能卡应用相关联的具体规则，那么，**SearchRuleFor(<AllDeviceApplications>, AID)**搜索的结果应该是“Never”（见“规则冲突处理”部分的说明）。

- 如果没有规则满足条件 a) 或 b)，继续搜索针对指定终端应用但针对所有电信智能卡应用的规则：

**SearchRuleFor(DeviceApplicationCertificate, <AllSEApplications>)**

如果规则存在，那么使用这条规则并停止搜索过程。

- 如果没有规则满足条件 a)、b) 或 c)，则搜索针对所有终端应用以及所有电信智能卡应用的

规则:

SearchRuleFor(<AllDeviceApplications>, <AllSEApplications>)

如果规则存在, 则使用这条规则。

#### 6.4.3.2 基于证书链的规则匹配

根据 6.4.2.2 节规定的“证书链中的下级证书优先级更高”的原则, 如果终端应用由证书链中的证书签名, 并且该证书链中超过一个证书有与之关联的访问控制规则, 那么, 应该使用与证书链中最低级别证书关联的规则。相应地, 在规则匹配过程中, 访问控制模块应按照该要求获取与证书链中适当的证书关联的访问控制规则。

访问控制模块应按如下步骤获取与证书链中适当的证书关联的访问控制规则。

a) 按照证书链中证书级别从低到高的顺序依次搜索与该证书及相应电信智能卡应用相关联的具体规则:

1) SearchRuleFor(EndEntityCertificate, AID)

如果规则存在, 则使用这条规则, 搜索停止。

2) SearchRuleFor(IntermediateCertificate<1>, AID)

如果规则存在, 则使用这条规则, 搜索停止。

...

3) SearchRuleFor(IntermediateCertificate<n>, AID)

如果规则存在, 则使用这条规则, 搜索停止。

4) SearchRuleFor(RootCertificate, AID)

如果规则存在, 则使用这条规则, 搜索停止。

b) 如果没有规则满足条件 a), 则搜索针对所有终端应用和指定电信智能卡应用的规则:

SearchRuleFor(<AllDeviceApplications>, AID)

如果规则存在, 则使用这条规则, 搜索停止。

c) 如果没有规则满足条件 a) 或 b), 搜索针对指定终端应用以及所有电信智能卡应用的规则:

1) SearchRuleFor(EndEntityCertificate, <AllSEApplications>)

如果规则存在, 则使用这条规则, 搜索停止。

2) SearchRuleFor(IntermediateCertificate<1>, <AllSEApplications>)

如果规则存在, 则使用这条规则, 搜索停止。

...

3) SearchRuleFor(IntermediateCertificate<n>, <AllSEApplications>)

如果规则存在, 则使用这条规则, 搜索停止。

4) SearchRuleFor(RootCertificate, <AllSEApplications>)

如果规则存在, 则使用这条规则, 搜索停止。

d) 如果没有规则满足条件 a)、b) 或 c), 搜索针对所有终端应用以及所有电信智能卡应用的规则:

SearchRuleFor(<AllDeviceApplications>, <All 电信智能卡 Applications>)

如果规则存在，则使用这条规则。

#### 6.4.4 访问控制流程

终端应用访问电信智能卡过程中，终端访问控制模块需要根据访问控制规则进行规则匹配，并根据规则匹配的结果判断是否允许终端应用的访问，相应的流程如图 3 所示。

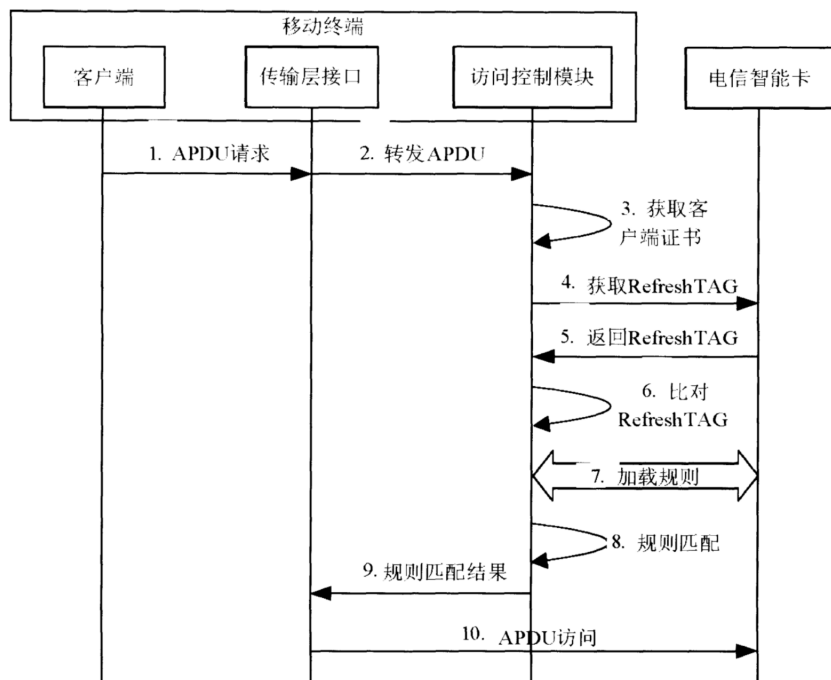


图 3 访问控制流程

流程说明如下：

1. APDU 请求：终端应用通过 SE-API 打开与电信智能卡应用交互的通信通道；
2. 转发 APDU：传输层 API 将终端应用发送的 APDU 请求转发给访问控制模块；
3. 获取终端应用证书：访问控制模块获取发起请求终端应用的签名证书，见 6.1 节的要求；
4. 获取 RefreshTAG：访问控制模块从规则库中获取更新标志（Refresh TAG）；
5. 返回 RefreshTAG：电信智能卡返回 RefreshTAG；
6. 比对 RefreshTAG：如果该标志与之前获取的数值不同，则进入下一步；否则跳到第 8 步；
7. 加载规则：按照“规则加载流程”重新从电信智能卡中读取规则，刷新终端缓存；
8. 规则匹配：访问控制模块基于终端应用签名证书的哈希值以及目标应用的 AID 匹配规则；
9. 规则匹配结果：将规则匹配的结果返回给传输层模块。如果规则匹配结果是不允许访问，则会向终端返回错误。如果访问许可，则返回授权执行的响应；
10. APDU 访问：如果允许终端应用访问，则电信智能卡访问接口发送 APDU 给电信智能卡。



## 附录 A

### (资料性附录)

#### 规则举例

本附录提供了电信智能卡存储的规则结构和内容示例，可供开发参考。为便于描述，以下示例中的 AID 采用 A0 00 00 01 51 xx 的格式，证书哈希值使用 111..., 222..., 333...等形式。

#### A.1 示例 1

示例中，访问控制条件如下：

AID1 = A0 00 00 01 51 01	-->access denied for all apps	
	-->conditions 1	
AID2 = A0 00 00 01 51 02	-->access allowed for 1 app (hash1)	
-->conditions 2		
AID3 = A0 00 00 01 51 03	-->access allowed for 1 app (hash1)	
-->conditions 2		
Any other AIDs	-->access allowed for all apps	-->conditions 3

以下为 PKCS#15 文件系统个性化后信息。

文件系统层次结构（基于文件系统）：

MF (3F00)

|-EF DIR (2F00) --> reference DF PKCS-15

|

|-DF PKCS-15 (7F50)

|-ODF (5031) --> reference DODF

|-DODF (5207) --> reference EF ACMain

|-EF ACMain (4200) --> reference EF ACRules

|-EF ACRules (4300) --> reference EF ACConditions...

|-EF ACConditions1 (4310)

|-EF ACConditions2 (4311)

|-EF ACConditions3 (4312)

文件系统层次结构（基于 PKCS#15 应用）：

PKCS#15 application (AID: A0 00 00 00 63 50 4B 43 53 2D 31 35)

|-ODF (5031) --> reference DODF

|-DODF (5207) --> reference EF ACMain

|-EF ACMain (4200) --> reference EF ACRules

|-EF ACRules (4300) --> reference EF ACConditions...

|EF ACConditions1 (4310)

|EF ACConditions2 (4311)

|EF ACConditions3 (4312)

#### EF DIR: 3F00/2F00

Based on this ASN.1 syntax:

```
DIRRecord ::= [APPLICATION 1] SEQUENCE {
  aid [APPLICATION 15] OCTET STRING,
  label [APPLICATION 16] UTF8String OPTIONAL,
  path [APPLICATION 17] OCTET STRING,
  ddo [APPLICATION 19] DDO OPTIONAL
}
```

aid PKCS-15 = A0 00 00 00 63 50 4B 43 53 2D 31 35

label = "PROVISIONING" = 50 52 4F 56 49 53 49 4F 4E 49 4E 47

path = 3F00/7F50

binary coding:

61 22 4F 0C A0 00 00 00 63 50 4B 43 53 2D 31 35 50 0C 50 52 4F 56 49 53 49 4F 4E 49 4E 47 51 04

3F 00 7F 50

#### ODF:

References file 5207.

Binary coding

A7 06 30 04 04 02 52 07

#### DODF:

GPAC OID(HEX encoding) = 2A 86 48 86 FC 6B 81 48 01 01

application name = "GP SE Acc Ctl" (example: value to be confirmed)

path to EF ACMain = 4200

binary coding:

A1 29 30 00 30 0F 0C 0D 47 50 20 53 45 20 41 63 63 20 43 74 6C A1 14 30 12 06 0A 2A 86 48 86 FC

6B 81 48 01 01 30 04 04 02 42 00

#### EF ACMain:

Refresh tag value is 01 02 03 04 05 06 07 08

path to EF ACRules = 4300

binary coding:

30 10 04 08 01 02 03 04 05 06 07 08 30 04 04 02 43 00

EF ACRules:

AID1 --> EFConditions 4310 --> access denied for all apps

AID2 --> EFConditions 4311 --> access allowed for 1 app (hash1)

AID3 --> EFConditions 4311 --> access allowed for 1 app (hash1)

\* --> EFConditions 4312 --> access allowed for all apps

binary coding:

30 10 A0 08 04 06 A0 00 00 01 51 01 30 04 04 02 43 10

30 10 A0 08 04 06 A0 00 00 01 51 02 30 04 04 02 43 11

30 10 A0 08 04 06 A0 00 00 01 51 03 30 04 04 02 43 11

30 08 82 00 30 04 04 02 43 12

EF ACConditions1: (access denied for all apps)

binary coding:

(empty file)

EF ACConditions2: (access allowed for 1 app)

Hash1 has the value 11

binary coding:

30 16 04 14 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11

EF ACConditions3: (access allowed for all apps)

binary coding:

30 0

## A.2 示例 2

示例中，访问控制条件如下：

AID1 = A0 00 00 01 51 01	-->access allowed for all apps	-->conditions 1
AID2 = A0 00 00 01 51 02	-->access allowed for 1 app (hash1)	-->conditions 2
AID3 = A0 00 00 01 51 03	-->access allowed for 3 apps (h1, h2, h3)	-->conditions 3
AID4 = A0 00 00 01 51 04	-->access denied for all apps	-->conditions 4
AID5 = A0 00 00 01 51 05	-->access denied for all apps	-->conditions 4
Any other AIDs	--> access denied for all apps	-->conditions 4

以下为 PKCS#15 文件系统个性化信息。

文件系统层次结构（基于文件系统）：

MF (3F00)

```

|-EF DIR (2F00) --> reference DF PKCS-15
|
|-DF PKCS-15 (7F50)
|-ODF (5031) --> reference DODF
|-DODF (5207) --> reference EF ACMain
|-EF ACMain (4200) --> reference EF ACRules
|-EF ACRules (4300) --> reference EF ACConditions...
|-EF ACConditions1 (4310)
|-EF ACConditions2 (4311)
|-EF ACConditions3 (4312)
|-EF ACConditions4 (4313)

```

文件系统层次结构（基于 PKCS#15 应用）：

PKCS#15 application (AID: A0 00 00 00 63 50 4B 43 53 2D 31 35)

```

|-ODF (5031) --> reference DODF
|-DODF (5207) --> reference EF ACMain
|-EF ACMain (4200) --> reference EF ACRules
|-EF ACRules (4300) --> reference EF ACConditions...
|-EF ACConditions1 (4310)
|-EF ACConditions2 (4311)
|-EF ACConditions3 (4312)
|-EF ACConditions4 (4313)

```

EF DIR: 3F00/2F00

Based on this ASN.1 syntax:

```

DIRRecord ::= [APPLICATION 1] SEQUENCE {
  aid [APPLICATION 15] OCTET STRING,
  label [APPLICATION 16] UTF8String OPTIONAL,
  path [APPLICATION 17] OCTET STRING,
  ddo [APPLICATION 19] DDO OPTIONAL
}

```

aid PKCS-15 = A0 00 00 00 63 50 4B 43 53 2D 31 35

label = "PROVISIONING" = 50 52 4F 56 49 53 49 4F 4E 49 4E 47

path = 3F00/7F50

binary coding:

61 22 4F 0C A0 00 00 00 63 50 4B 43 53 2D 31 35 50 0C 50 52 4F 56 49 53 49 4F 4E 49 4E 47 51 04

3F 00 7F 50

ODF:

References file 5207.

binary coding:

A7 06 30 04 04 02 52 07

DODF:

GPAC OID(HEX encoding) = 2A 86 48 86 FC 6B 81 48 01 01

application name = "GP SE Acc Ctl" (example: value to be confirmed)

path to EF ACMain = 4200

binary coding:

A1 29 30 00 30 0F 0C 0D 47 50 20 53 45 20 41 63 63 20 43 74 6C A1 14 30 12 06 0A 2A 86 48 86 FC  
6B 81 48 01 01 30 04 04 02 42 00

EF ACMain:

Refresh tag value is 01 02 03 04 05 06 07 08

path to EF ACRules = 4300

binary coding:

30 10 04 08 01 02 03 04 05 06 07 08 30 04 04 02 43 00

EF ACRules:

AID1 --> EFConditions 4310 --> access allowed for all apps

AID2 --> EFConditions 4311 --> access allowed for 1 app (h1)

AID3 --> EFConditions 4312 --> access allowed for 3 apps (h1, h2, h3)

AID4 --> EFConditions 4313 --> access denied for all apps

AID5 --> EFConditions 4313 --> access denied for all apps

\* --> EFConditions 4313 --> access denied for all apps

binary coding:

30 10 A0 08 04 06 A0 00 00 01 51 01 30 04 04 02 43 10  
30 10 A0 08 04 06 A0 00 00 01 51 02 30 04 04 02 43 11  
30 10 A0 08 04 06 A0 00 00 01 51 03 30 04 04 02 43 12  
30 10 A0 08 04 06 A0 00 00 01 51 04 30 04 04 02 43 13  
30 10 A0 08 04 06 A0 00 00 01 51 05 30 04 04 02 43 13  
30 08 82 00 30 04 04 02 43 13

EF ACConditions: (access allowed for all apps)

binary coding:

30 00

EF ACConditions: (access allowed for 1 app)

binary coding:

30 16 04 14 11

EF ACConditions: (access allowed for 3 apps)

binary coding:

30 16 04 14 11

30 16 04 14 22

30 16 04 14 33

EF ACConditions: (access denied for all apps)

binary coding:

(empty file)

### A.3 示例 3

示例中，访问控制条件如下：

Default AID                      -->access allowed for 1 app (hash0)    -->conditions 1

AID1 = A0 00 00 01 51 01    -->access allowed for 1 app (hash1)    -->conditions 2

AID2 = A0 00 00 01 51 02    -->access allowed for 1 app (hash2) + APDU Filter -->conditions 3

AID3 = A0 00 00 01 51 03    -->access allowed for all apps        -->conditions 4

以下为 PKCS#15 文件系统个人化信息。

文件系统层次结构（基于文件系统）：

MF (3F00)

|-EF DIR (2F00) --> reference DF PKCS-15

|

|-DF PKCS-15 (7F50)

|-ODF (5031) --> reference DODF

|-DODF (5207) --> reference EF ACMain

|-EF ACMain (4200) --> reference EF ACRules

|-EF ACRules (4300) --> reference EF ACConditions...

|-EF ACConditions1 (4380)

|-EF ACConditions2 (4381)

|-EF ACConditions3 (4382)

|EF ACConditions4 (4383)

文件系统层次结构（基于 PKCS#15 应用）：

PKCS#15 application (AID: A0 00 00 00 63 50 4B 43 53 2D 31 35)

|ODF (5031) --> reference DODF

|DODF (5207) --> reference EF ACMain

|EF ACMain (4200) --> reference EF ACRules

|EF ACRules (4300) --> reference EF ACConditions...

|EF ACConditions1 (4380)

|EF ACConditions2 (4381)

|EF ACConditions3 (4382)

|EF ACConditions4 (4383)

EF DIR: 3F00/2F00

Based on this ASN.1 syntax:

```
DIRRecord ::= [APPLICATION 1] SEQUENCE {  
  aid [APPLICATION 15] OCTET STRING,  
  label [APPLICATION 16] UTF8String OPTIONAL,  
  path [APPLICATION 17] OCTET STRING,  
  ddo [APPLICATION 19] DDO OPTIONAL  
}
```

aid PKCS-15 = A0 00 00 00 63 50 4B 43 53 2D 31 35

label = "PROVISIONING" = 50 52 4F 56 49 53 49 4F 4E 49 4E 47

path = 3F00/7F50

binary coding:

61 22 4F 0C A0 00 00 00 63 50 4B 43 53 2D 31 35 50 0C 50 52 4F 56 49 53 49 4F 4E 49 4E 47 51 04

3F 00 7F 50

ODF:

References file 5207.

binary coding:

A7 06 30 04 04 02 52 07

DODF:

GPAC OID(HEX encoding) = 2A 86 48 86 FC 6B 81 48 01 01

application name = "GP SE Acc Ctl" (example: value to be confirmed)

path to EF ACMain = 4200

binary coding:

A1 29 30 00 30 0F 0C 0D 47 50 20 53 45 20 41 63 63 20 43 74 6C A1 14 30 12 06 0A 2A 86 48 86 FC  
6B 81 48 01 01 30 04 04 02 42 00

EF ACMain:

Refresh tag value is 01 02 03 04 05 06 07 08

path to EF ACRules = 4300

binary coding:

30 10 04 08 01 02 03 04 05 06 07 08 30 04 04 02 43 00

EF ACRules:

Default AID --> EFConditions 4380 --> access allowed for 1 app (h0)

AID1 --> EFConditions 4381 --> access allowed for 1 app (h1)

AID2 --> EFConditions 4382 --> access allowed for 1 app (h2)...

AID3 --> EFConditions 4383 --> access allowed for all apps

binary coding:

30 08 81 00 30 04 04 02 43 80

30 10 A0 08 04 06 A0 00 00 01 51 01 30 04 04 02 43 81

30 10 A0 08 04 06 A0 00 00 01 51 02 30 04 04 02 43 82

30 10 A0 08 04 06 A0 00 00 01 51 03 30 04 04 02 43 83

EF ACConditions: (access allowed for 1 app)

Hash0 has the value 000...

binary coding:

30 16 04 14 00

EF ACConditions: (access allowed for 1 app)

Hash1 has the value 11

binary coding:

30 16 04 14 11

EF ACConditions: (access allowed for 1 app)

Hash2 has the value 222...

APDU filter : 80 F2 00 00 / FF FF FF FF + 80 CA 00 00 / FF FF 00 00

NFC event : NEVER

binary coding:

30 35 04 14 22 A0 1D A0 16 A1 14 04 08 80



YD/T 3202—2016

F2 00 00 FF FF FF FF 04 08 80 CA 00 00 FF FF 00 00 A1 03 80 01 00

EF ACConditions: (access allowed for all apps)

binary coding:

30 00

---

中华人民共和国通信行业标准  
移动通信终端访问电信智能卡  
安全技术要求  
YD/T 3202—2016

\*

人民邮电出版社出版发行  
北京市丰台区成寿寺路 11 号邮电出版大厦  
邮政编码：100064  
北京康利胶印厂印刷  
版权所有 不得翻印

\*

开本：880×1230 1/16 2017 年 6 月第 1 版  
印张：2 2017 年 6 月北京第 1 次印刷  
字数：48 千字

15115 • 1234

定价：20 元

本书如有印装质量问题，请与本社联系 电话：(010)81055492