Advanced Card Systems Ltd.
Card & Reader Technologies

ACOSJ-G
【接触式】

功能规格书 V2.04

info@acs.com.hk
www.acs.com.hk

目录

图目录

表目录

1.0. 概览

ACOSJ 是龙杰智能卡有限公司（Advanced Card Systems Ltd.，ACS）自主研发的智能卡操作系统。它基于 JAVA 卡虚拟机进行操作，功能配置符合 GlobalPlatform Card Specification（版本 2.2.1）、JAVA Card Specification（ 版本 3.0.4）和 Mapping Guidelines（版本 1.0.1）。

本文件旨在详细介绍 ACOSJ 智能卡操作系统的特性和功能。

1.1. ACOSJ-G 版本

版本	发布日期	修订
ACOSJ v1.01	2015 年 6 月	• 40KB EEPROM • 工作电压：2.7V - 5.5V
ACOSJ v2.00	2018 年 5 月	• 95KB EEPROM • 工作电压：2.1 V - 5.5 V • 更改配置内存地址
ACOSJ v2.04	2019 年 4 月	• 95KB EEPROM • 工作电压：2.1 V - 5.5 V • 更改配置内存地址 • 功能增强

表1 ：修改历史

•

1.2. 符号和缩写

缩写	说明
AES	高级加密标准 (Advanced Encryption Standard)
AID	应用标识符 (Application Identifier)
APDU	应用协议数据单元 (Application Protocol Data Unit)
API	应用程序编程接口 (Application Programming Interface)
ASCII	美国信息互换标准代码 (American Standard Code for Information Interchange)
ATR	复位应答 (Answer-to-Reset)
ATQ	复位应答（针对非接触卡）(Answer-to-Request)
BCD	二进制编码的十进制 (Binary Coded Decimal)
BER	基本编码规则 (Basic Encoding Rules)
CAT	卡应用工具包/ 加密授权模板 (Card Application Toolkit; or Cryptographic Authorization Template)
CBC	密码块链接 (Cipher Block Chaining)
CCT	加密校验和控制引用模板 (Control Reference Template for Cryptographic Checksum)

缩写	说明
CIN	卡片图像号码/卡片识别号码 (Card Image Number/Card Identification Number)
CLA	命令报文的类字节 (Class byte of the command message)
CRT	控制引用模板(Control Reference Template)
CT	加密控制引用模板 (Control Reference Template for Confidentiality)
CVM	持卡人验证方法 (Cardholder Verification Method)
DAP	数据鉴别模式 (Data Authentication Pattern)
DEK	数据加密密钥 (Data Encryption Key)
DER	唯一编码规则 (Distinguished Encoding Rules)
DES	数据加密标准 (Data Encryption Standard)
DST	数字签名控制引用模板 (Control Reference Template for Digital Signature)
ECB	电子源码书 (Electronic Code Book)
EMV	欧陆卡 Europay、万事达卡 MasterCard®与威士卡（VISA®）；指支付系统的 IC 卡规范
ENC	加密 (Encryption)
FCI	文件控制信息 (File Control Information)
HEX	十六进制 (Hexadecimal)
HMAC	密钥相关的哈希运算消息认证码 (Keyed-Hash Message Authentication Code)
ICC	集成电路卡 (Integrated Circuit Card)
ICV	初始链表向量 (Initial Chaining Vector)
IIN	发卡方识别码 (Issuer Identification Number)
INS	命令报文的指令字节
ISO	国际标准化组织 (International Organization for Standardization)
Lc	情形 3 或情形 4 命令中数据的精确长度
Le	情形 2 或情形 4 命令响应中数据的最大长度
LV	长度值 (Length Value)
MAC	报文认证码 (Message Authentication Code)
MEL	Multos 可执行语言 (MULTOS Executable Language)；MULTOS™运行环境指令集。
OID	对象识别码 (Object Identifier)
P1	引用控制参数 1
P2	引用控制参数 2
PIN	个人识别码 (Personal Identification Number)
PKI	公钥基础设施 (Public Key Infrastructure)

缩写	说明
RAM	随机存取存储器 (Reserved for Future Use)
RFU	保留为将来使用 (Reserved for Future Use)
RID	注册应用提供商标识 (Registered Application Provider Identifier)
ROM	只读存储器 (Read-only Memory)
RSA	RSA 非对称算法 (Rivest/Shamir/Adleman asymmetric algorithm)
SCP	安全通道协议/ （欧洲电信标准协会）智能卡平台 (Secure Channel Protocol; or (ETSI) Smart Card Platform)
SW	状态字 (Status Word)
SW1	状态字 1 (Status Word One)
SW2	状态字 2 (Status Word Two)
TLV	标签长度值 (Tag Length Value)
TP	信任点 (Trust Point)
'xx'	使用单引号标出的十六进制数表示十六进制值
'X'	表内单元格列出的值，其作用在'含义'一栏列出
'-'	表内单元格所含值（0 或 1），该值不影响表格对应行给出的‘含义’。

表2:符号和缩写

2.0. 卡片规格

本节概述了 ACOSJ-G 的特性和功能。

2.1. 电气参数

- 工作电压（ACOSJ-G v1.01）：
  - 2.7 V – 5.5 V 源电压
- 工作电压（ACOSJ-G v2.04）：
  - 2.1 V – 5.5 V 源电压
- 最大外部时钟频率：10 MHz
- 最大 CPU 时钟频率：28 MHz
- ESD 保护：大于 5 kV (HBM)

2.2. 环境规格

- 工作温度：-25° C – +85° C

2.3. 通信协议

- T=0和T=1，最高625 kbps波特率（外部时钟频率5MHz）

2.4. 内存

- 容量：95 KB (ACOSJ-G 2.04), 40 KB (ACOSJ-G 1.01)
- EEPROM 耐久性：50 万次檫写（25° C）
- 数据存储时间：30 年（25° C）

2.5. 加密功能

- DES, 2K3DES, 3K3DES (ECB 和 CBC)
- AES:128/192/256 位(ECB 和 CBC)
- RSA:768 – 2048 位
- ECC:模数 112/128/160/192/224/256/384 位
- Hash: SHA1, SHA224, SHA256, SHA384, SHA512
- SM2/SM3/SM4
- SEED:128 位

2.6. 符合标准

- 符合 ISO 7816 第 1、2、3 和 4 部分
- 符合 JAVA Card Specification（3.0.4 版）
- 符合 Global Platform Specification（2.2.1 版）
- 符合 Mapping Guidelines 1.0.1 标准

2.7. 复位应答（ATR，接触式卡）

卡片复位（例如：上电）后，会按照 ISO 7816 第 3 部分规定传送复位应答（ATR）。ACOSJ 支持正向和反向约定的接触式 T=0 和 T=1 协议。

以下是默认的 ATR：

参数	ATR	说明
TS	3Bh	正向约定，首先发送最低有效位
T0	69h	TB1、TC1 和 TD1 存在，跟随 9 个历史字符
TB1	00h	无需额外编程电压
TC1	02h	额外保护时间
9 个历史字符（ACOSJvXXX）		

表3 ：ATR 配置

9 个历史字节的构成如下：

历史字节	ATR	说明
T1	41h	表示“A”
T2	43h	表示“C”
T3	4Fh	表示“O”
T4	53h	表示“S”
T5	4Ah	表示“J”
T6	76h	表示“V”
T7~T9	31h 30h 31h 或 32h 30h 34h	表示“101” 或 表示“204”

表4 ：ATR 的历史字节

3.0. 卡片周期状态

ACOSJ 具有五种卡片状态： OP_READY 、 INITIALIZED 、 SECURED 、 CARD_LOCKED 和 TERMINATED，如下图所示：

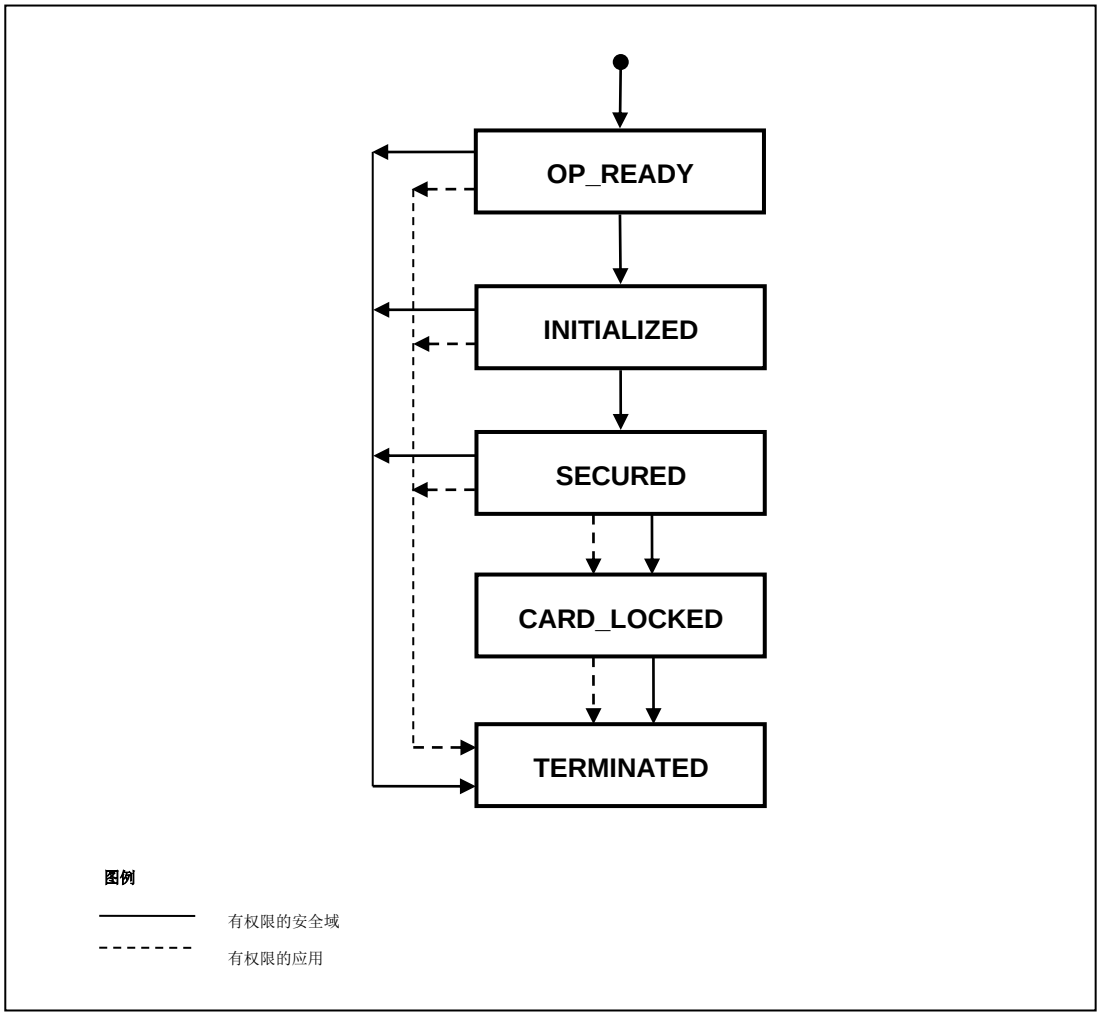

图1:卡片生命周期

3.1. OP_READY

OP_READY 状态表明运行时环境已经可以使用，发卡方安全域作为当前被选定的应用，可以接收、执行和响应 APDU 命令了。

卡片处于 OP_READY 状态时，以下功能可用：

- 运行时环境为执行做好准备；
- OPEN 为执行做好准备；
- 发卡方安全域默认成为所有卡片接口的选中应用；
- 存放在不可变永久内存里的可执行装载文件被注册在 GP 注册表中；
- 发卡方安全域里的初始密钥可用。

可以更改卡片内容，加载的装载文件允许含有卡内不存在的应用。

可以从可执行的装载文件安装任何应用。

此外，如果该阶段有任意可用的个人化信息，都可以进行应用个人化。

OP_READY 状态可以被卡外实体用来执行下面的动作：

- 加载和/或安装附加安全域。
- 为了维护一个与发卡方安全域相独立的加密密钥，安全域密钥可以被插入（安装）。

3.2. INITIALIZED

INITIALIZED 状态是一个可管理的卡产品状态。从 OP_READY 状态进入 INITIALIZED 状态的卡生命周期状态的迁移是不可逆的。该状态的功能超出了本规格书的描述范围。这个状态表示一些初始的数据已经组装（比如：发卡方安全域密钥和/或数据），但是该卡还不能发给卡持有者。

3.3. SECURED

SECURED 状态是卡发行后趋向于操作的卡生命周期状态。在该状态下，安全域和应用可以实施各自的安全策略。从 INITIALIZED 到 SECURED 的状态迁移是不可逆的。

SECURED 状态应该用于向卡外实体表明发卡方安全域包含了全部功能所需要的所有密钥和安全元素。

3.4. CARD_LOCKED

卡生命周期状态 CARD_LOCKED 为卡发卡方提供了禁止选择安全域和应用的功能的能力。从 SECURED 到 CARD_LOCKED 的卡生命周期状态的迁移是可逆的。

卡片设置为 CARD_LOCKED 状态表示仅可选中具有最终应用权限的应用。

该状态不允许更改卡片内容，不能进行任何数据管理（具体包括安全域密钥和数据）。

OPEN 或具有卡锁权限的安全域或具有卡锁权限的应用可以发起从 SECURED 到 CARD_LOCKED 状态的迁移。

3.5. TERMINATED

TERMINATED 状态表明卡的生命周期和卡的终止。从任何其它状态到 TERMINATED 状态的迁移都是不可逆的。

TERMINATED 状态永久性终止卡片的所有功能，包括卡片所有的内容管理和生命周期更改。检测到极端安全威胁或卡片到期时， 应用可以在该状态下从逻辑上'销毁'卡片。如果安全域具有最终应用权限，则只能处理 GET DATA 命令，本规格书中定义的所有其他命令均被禁用或运行返回异常。如果应用具有最终应用权限，命令处理与发卡方策略有关。

OPEN 自身，或具有卡片终止权限的安全域，或具有卡片终止权限的应用可以发起从任意状态到 TERMINATED 状态的转换。

4.0. 卡片架构

ACOSJ 卡为符合 GP 规范的 Java 卡，其应用系统的组织架构如下图所示：

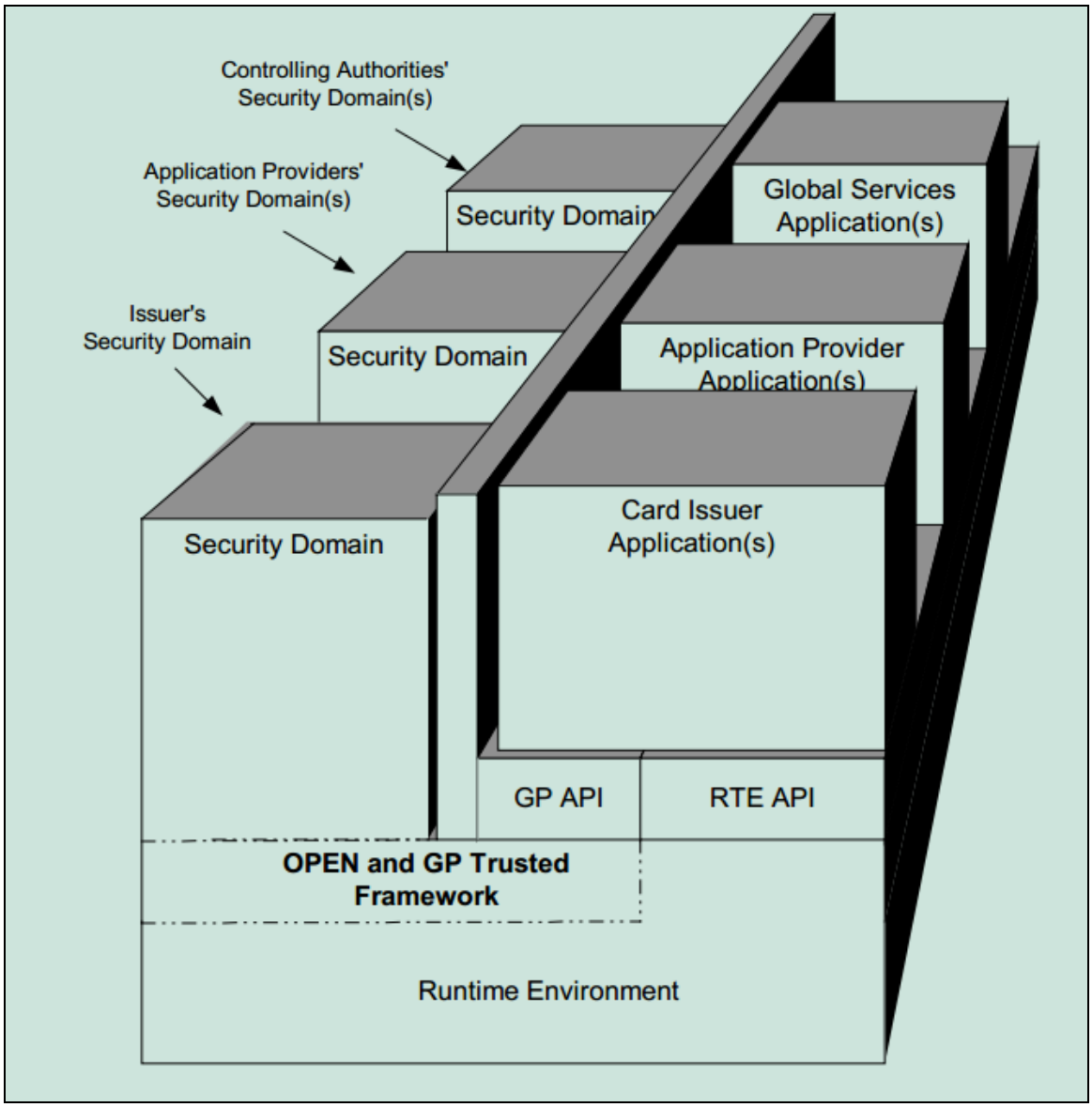

图2 :ACOSJ 系统架构

5.0. GP APDU 命令参考

本章主要描述被实现的 GlobalPlatform APDU 命令。这些命令按照字母顺序列出。

表 5 总结了发卡方安全域支持的 APDU 命令，以及其他安全域支持这些命令时需满足的要求。当支持逻辑通道时，管理通道命令只能被 OPEN 处理，并且不需要安全域对此命令进行支持。

命令	OP_READY			INITIALIZED			SECURED			CARD_LOCKED		TERMINATED	
	AM SD	DM SD	SD	AM SD	DM SD	SD	AM SD	DM SD	SD	FASD	SD	FASD	SD
删除可执行的装载文件													
删除可执行的装载文件和相关应用													
删除应用	✓			✓			✓						
删除密钥													
获取数据	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
获取状态	✓			✓			✓			✓			
安装[针对加载]													
安装[针对安装]													
安装[针对加载、安装和使文件可选]													
安装[针对安装和使文件可选]	✓	✓		✓	✓		✓	✓					
安装[针对使文件可选]													
安装[针对引渡]													
安装[针对注册表更新页面]													
安装[针对个人化]													
加载													
重装密钥	✓			✓			✓						
选择	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
设置状态	✓			✓			✓			✓			
存储数据	✓			✓			✓						

表5:卡片各个生命周期状态中被认证的 GlobalPlatform 命令

AM SD 具有授权管理权限的安全域。

DM SD 具有委托管理权限的安全域。

FA SD 具有最终应用权限的安全域。

注： *命令是否支持具有最终应用权限的应用（非安全域），首先受到卡片生命周期状态的限制，其次与发卡方政策有关。*

SD 其他安全域。

✓ 必须支持。

空白格 可选支持。

阴影格 禁止支持。

表 6 总结了 APDU 命令的最低安全要求。

命令	最小安全级别
删除	确保通道初始化或数字签名验证的安全性
获取数据	无
获取状态	确保通道初始化的安全性
安装	确保通道初始化或数字签名验证的安全性
加载	确保通道初始化或数字签名验证的安全性
管理通道	不适用
重装密钥	确保通道初始化的安全性
选择	不适用
设置状态	确保通道初始化的安全性
存储数据	确保通道初始化的安全性

表6 :GlobalPlatform 命令的最低安全要求

5.1. 删除命令

用于删除唯一可识别的对象，例如可执行的装载文件、应用、可执行的装载文件及相关应用或密钥。待删除的对象必须是选中应用能够唯一标识的。

5.2. 获取数据命令

用来取得单一的数据对象（可以是被构建的对象），或者是一系列的数据对象。引用控制参数 P1 和 P2 编码用于定义指定的数据对象标签。数据对象可能含有密钥相关信息。

5.3. 获取状态命令

根据给定的匹配/查询条件获取发卡方安全域、可执行的装载文件、可执行模块、应用或安全域生命周期状态信息。

5.4. 安装命令

发送至安全域的安装命令用于初始化或执行卡片内容管理所需的各个步骤。

5.5. 加载命令

本小节定义了加载命令数据域传输的装载文件的结构，用以完成装载文件的加载。ICC 的内部处理或装载文件的存储超出了本规格书的描述范围。

可以使用多个加载命令将一个装载文件传输至卡片。这个装载文件被分成多个便于传输的小块。每一个加载命令的编号是从 00h 开始的。加载命令的编号必须严格按照顺序逐一递增。装载文件的最后一个数据块传输完成后将通知卡片。

当接收到装载文件的最后一块后，卡将执行先于加载命令的对装载文件必要的内部处理和在安装[针对加载]命令中标识的任何附加的处理。

5.6. 管理通道命令

该命令是由卡上已经获知逻辑通道的 OPEN 域处理的，这个命令用来打开和关闭辅助的逻辑通道。基本逻辑通道（通道号为 0）永远不会关闭。

5.7. 重装密钥命令

该命令用于：

- 用一个新的密钥替换一个已经存在的密钥，新密钥与当前密钥 ID 务必相同，但是新密钥与当前密钥的版本号可以相同或者不同。
- 使用多个新密钥取代多个当前密钥：新密钥与当前密钥 ID 务必相同，但是新密钥与当前密钥的版本号可以相同或者不同（所有新密钥的版本号相同）；
- 添加单个新密钥：新密钥具有与当前密钥不同的密钥 ID/密钥版本号组合；
- 添加多个新密钥：新密钥具有与当前密钥不同的密钥 ID/密钥版本号组合（所有新密钥的密钥 ID/密钥版本号组合相同）；

密钥管理操作需要多次运行重装密钥命令时，建议使用多个重装命令的命令链以保证操作的完整性。

在这个规范版本中，非对称密钥的公开值是通过明文表现（传送）的。

5.8. 选择命令

用于选择应用。OPEN 仅仅处理已经设置了 SELECT [by name]选项的选择命令。SELECT [by name]选项之外的所有其他选项将被转至指定逻辑通道内当前选中的安全域或应用。

5.9. 设置状态命令

用于修改卡片或应用的生命周期状态。

5.10. 存储数据命令

用来传输数据给处理这个命令的应用或安全域。

根据先前接收的命令，安全域会决定该命令是发送给安全域自身或应用。如果先前收到了安装[针对个人化]命令，存储数据命令是发送给应用的。

使用多个存储数据命令将数据发送给应用或安全域时，传输过程中会将数据分成多个小块。最后一个数据块传输完成后将通知安全域。

安全域接收有效的安装[针对个人化]命令（“有效”是指该命令指定了一个应用，条件是安全域须将连续接收的存储数据命令转发给这个应用）后将开始执行个人化会话。

个人化会话的终止条件：

- 卡片复位；
- 取消选定安全域（例如，同一个逻辑通道中选择了另一个或者同一个 Applet）；
- 此安全域在同一个或另一个逻辑通道中被选中；
- 安全域建立的安全通道会话（如果存在）被重置，可能是被目标应用重置；
- 安全域收到了安装[针对个人化]命令（为另一个应用开始新的个人化会话）；
- 安全域收到存储数据命令，指定 P1. b8=1（最后一个数据块）；

个人化会话外接收的任意存储数据命令将由安全域自己处理。

6.0. GlobalPlatform API

6.1. GlobalPlatform 在 JAVA 卡上

本章仅描述 GlobalPlatform 2.2.x Java 卡要求的 API。Open Platform 2.0.1 的 API 的使用一直允许支持旧版应用，但是被弃用了。规范的 2.1.1 版本里有定义。

如果可用的话，旧版 API 和新版 API 可能会访问的同一个对象，这对在两个类中具有相同名称的方法来说是显而易见的（例如：setATRHistBytes(), setCardContentState()和 getCardContentState()），还需要注意的是，举个例子来说，一个新应用通过 UPDATE()方法改变全局 PIN 的值，会影响到另一个应用调用弃用的方法 setPIN()对相同的 PIN 的进行的验证。

GlobalPlatform 特定的要求

为了保证 GlobalPlatform 实现的更高的互用性，GlobalPlatform 也采用了 Java 卡™ 2.2.x 虚拟机规范第 6.2 小节安装中定义的顺序。

GlobalPlatform 的实施对 Java 卡™ 2.1.1 运行环境（JCRE）规范 和 Java 卡™ 2.1.1 应用编程接口的标准功能稍有改动：部分更改与新版的 Java 卡™ 2.2.x 规范一致了，不再算是修改。

为了实现共享访问，Java Card™ 2.2.x 运行环境（JCRE）规范 第 6.2.4 小节规定将 GPRegistryEntry 对象部署为可共享接口对象。

GlobalPlatform 包的 AID

每一个 GlobalPlatform 包的 AID 都将是一个 RID 和一个 PIX 的串联。基于附录 H- GP 的数据及卡的识别数据中指定的 RID 的新的 GP API（GP2.1 和 GP2.1.1 一样）的 Java 卡导出文件的 AID 是 'A00000015100'。

安装

根据 Java 卡™ 2.2.x 运行环境 (JCRE)规范 第 3.1 小节- install 方法，被传递给方法的参数定义为初始化参数，它来自输入的字节数组参数中的内容。

本规范扩展了以上要求的内容，进一步定义了安装参数的内容，将同时影响 OPEN 的实现以及为 GlobalPlatform 卡而研发的 Java 卡 Applet 的操作。然而，不会影响 Java 卡™ 2.1.1 应用编程接口 规范关于 Applet 类中 install()方法的定义。

安装参数会标识出安装[针对安装]命令中出现的如下数据（参见小节 5.5.2.3.2 - 安装[针对安装]命令的数据域）：

- 实例 AID；
- 权限；
- 应用指定参数[1]。

[1] *APDU 命令包含代表 TLV 编码系统的安装参数以及应用指定参数，应用只需要获知应用指定参数，即只将 TLV 编码结构'C9'的 LV 部分看做应用指定参数。*

OPEN 负责确保参数（bArray、bOffset 和 bLength）含有下列信息：

数组 bArray 须包含以下连续的 LV 编码数据：

- 实例 AID 的长度；
- 实例 AID；
- 权限的长度；
- 权限；
- 应用指定参数的长度；
- 应用指定参数。

字节 bOffset 须包含数组内指向实例 AID 长度的偏移量。

字节 bLength 须包含表示数组中上述定义数据总长度的长度值。

调用 Java 卡™ 2.1.1 应用编程接口规范中 Applet 类的 register (byte [] bArray, short bOffset, byte bLength) 方法时，Applet 必须使用实例 AID 作为参数。

T=0 传输协议

GlobalPlatform 卡要求能够在多种环境中使用（如读卡设备）。目前，Java 卡™ 2.1.1 运行环境（JCRE）规范 和 Java Card™ 2.2.x 运行环境（JCRE）规范 描述的情形 2 命令（当使用 T=0 协议时）行为与 EMV2000 相矛盾。GlobalPlatform 强制规定 JCRE 必须依照 ISO/IEC 7816 处理该情况的命令：接收情况 2 命令的 Applet 做出反应并调用适当的 API 输出数据。如果数据长度小于终端期望收到的长度，OPEN 将存储数据，输出'6Cxx'响应码，并等待 CAD 重新发送长度正确的命令。收到重新发送的命令后，JCRE 将管理存储数据的输出。

原子操作

除非另有规定，GlobalPlatform API 的所有内部永久对象必须遵从正在进行中的事务。

该 API 执行的所有操作，除了 Application.processData()方法，都必须符合原子性原则。负责实施速度检查的对象不必遵从正在进行的事务。

逻辑通道

以下逻辑通道限制条件适用于 Java 卡™ 2.2.x（具体请参见 Java 卡™ 2.2.x 运行环境（JCRE）规范）：

根据小节 6.3 命令调度 的定义，在逻辑通道上选择应用的操作在以下情况下将失败：

相同的应用或其它在同一个包（将被选定的应用被实例化时）中的已被实例化的应用在另一个逻辑通道上当前是被选定的，但是应用的代码没有实现 MultiSelectable 接口。安全域必须实现 MultiSelectable 接口。

根据小节 7.3.3 - 个人化支持 的定义，将情境从安全域更改到应用的操作在以下情况下将失败：

相同的应用或从同一个包（这个将被个人化的应用实例化时的包）中实例化的其它的应用当前已经在其它的逻辑通道上被选定，但是应用的代码没有实现 MultiSelectable 接口。

一个应用如果具有缺省被选择的权限并且要在一个支持附加逻辑通道的卡上运行的话，那它必须实现 MultiSelectable 接口。

GlobalPlatform 只通过卡定义逻辑通道号的分配。做为 Java Card 2.2 定义的一项可选的特性，卡也可以通过终端支持逻辑通道号的分配。

加密算法

支持 RSA 加密的 GlobalPlatform 卡将支持密钥构造者 Key Builder 类中没有定义的密钥长度。密钥长度的更多特殊的支持将是可用的，但是，这个密钥长度是 4 字节（32 位）的倍数并且是在实现所定义允许的密钥长度范围内的。

信任级别

Java 卡规范 2.2.x 版利用数据包 AID 的 RID、Applet 和实例来保障这些机构间的信任级别。Java 卡™ 2.1.1 应用编程接口 4.2.2 小节 - AID 用法 定义了组件 AID 的 RID 必须匹配数据包 AID 的 RID。而且，根据 Java 卡™ 2.2.x 应用编程接口 规范对 register (byte [] bArray, short bOffset, byte bLength) 方法的定义，如果 bArray 参数中 AID 字节的 RID 部分不匹配 Applet 的 Java 卡名称中的 RID 部分，必须抛出异常。

从实际实施的视角，强制实例 AID 的 RID 必须与实例化源组件的 RID 相同的要求并不实际。GlobalPlatform 并不强制要求实例 AID 及其原始数据包之间存在任何连接（不要求实例 AID 和原始数据包 AID 之间有连接）。然而，同一数据包内所有应用必须享有同等信任度。

GlobalPlatform 方法的调用

为 GlobalPlatform 卡开发的任意 Java 卡 Applet 均可访问此处定义的应用编程接口，但也有限制条件，该限制与 Applet 的构造器以及 Java Card™ 2.2.x 应用编程接口 中 Applet 类的 install()方法相关。本规范未明确定义 Applet 实例何时成为卡片 GlobalPlatform 注册表项，Applet 开发商只能假设发生于 install()方法成功完成之后。为了保证互操作性，如果 GlobalPlatform API 方法需要访问调用发起方 Applet 的 GlobalPlatform 注册表项，则不能从构造器内或 install()方法调用该 API 方法。

以下是可以从构造器内或 install()方法调用的方法列表：

- getCardState;
- getCVM;
- getService

如果应用错误地调用 org.globalplatform.GPSystem 类中除了以上所列的方法外的方法时，发生这种错误时要求卡片如何操作，例如要求卡片抛出异常或者处理 install()方法，相关要求尚未定义。

选择

在 GlobalPlatform 卡上，如果 select()方法处理过程发生异常，或 select()方法返回错误，或由于应用没有实施 Multiselectable 接口而导致应用不能选中，OPEN 继续搜索 GlobalPlatform 注册表，以寻找下一个完全或部分符合 6.4.2.1.2 小节定义的匹配应用。如果没有选择任何应用，响应逻辑通道保持开放（没有当前选中应用）。如果没有应用被选定，这样将导致相应的逻辑通道打开，但是没有当前选定的应用。由于当前没有应用被选定，除了管理通道命令和选择命令以外任何后续的命令都将被拒绝。卡外实体应当针对这样的错误采取相应的动作，比如，选择其它应用，关闭相应的逻辑通道，复位或下电卡。

GlobalPlatform Java 卡™ API 说明书的方法概要和细节现在可用于一个单独的文档这可以在 GlobalPlatform 网站里找到。

7.0. 预个人化

IC 首次上电时处于预个人化状态。

在预个人化状态，首先需要发送 INIT_CARD 命令来使用默认值初始化卡片内存区。然后再通过 ACOSJ ROOT 应用将关键的系统数据（例如"ATR"、"ATS"等）存储到 EEPROM 中。数据加载完毕并确认不会进一步更改后，必须执行命令来禁用 ACOSJ ROOT 应用。

IC 成功执行 Active Card 命令退出预个人化状态后，如果没有设置为其它生命周期状态，则默认处于 GlobalPlatform 卡片生命周期的 OP_READY 状态。

一旦成功执行了 Active Card 命令，就无法返回到预个人化状态。

7.1. 预个人化流程

请求 ATR 之后，必须使用芯片传输密钥才能访问 ACOSJ Root 应用。

如果没有初始化 IC，则必须执行下列步骤来初始化 IC。

1. 请求 ATR。
2. INIT_CARD 命令。
3. 请求 ATR。

IC 初始化后，可以用作 GlobalPlatform 卡进行测试。

如果 IC 已经初始化，则必须执行以下步骤：

1. 请求 ATR。
2. SELECT 命令选择 ACOSJ Root 应用。
3. INIT_CARD 命令。
4. 根据需要，可以多次使用 READ）和 WRITE 命令。
5. 用户确认无需进一步更改关键系统数据（例如"ATR"、"ATS"等）后，必须发送 ACTIVE 命令。
6. 重启卡片，

注：传输密钥也是 ACOSJ Root 应用的预个人化密钥，必须向 ACS 索取。

8.0. ACOSJ ROOT 应用

8.1. ACOSJ ROOT 应用描述

ROOT 应用命令只有在正确选择了传输密钥后才能操作。当进入 ROOT 应用后，用户可以通过 ROOT 应用所支持的一些命令来读取或配置卡片的参数。如果要退出 ROOT 应用而选择其他应用，必须重新复位卡片。

ROOT 应用下可以读取或配置卡片的各种参数。

ROOT 应用在卡片激活状态下将会失效。

8.2. ACOSJ ROOT 应用命令参考

8.2.1. INIT_CARD 命令

这是一个重置卡片的命令。由于该命令是初始化整个 EEPROM，所以该命令执行时间大约需要 5S.

8.2.2. 读取命令

这是一个读取配置区的命令。可以通过它读取卡片的一些配置参数信息。

8.2.3. 写入命令

这是一个写配置区的命令。 可以通过它设置卡片的一些配置参数信息。

8.2.4. 激活命令

这是一个激活命令。该命令一旦执行成功后，BOOT 应用将会失效，也不能再直接读取或设置卡片的配置参数.

9.0. ACOSJ IDENTIFY 应用

9.1. ACOSJ IDENTIFY 应用描述

使用选择命令选择 IDENTIFY 应用(AID 为 6163732E636F732E61636F736A766572)后，ACOSJ 将会返回卡片的版本及是否激活信息。

9.2. ACOSJ IDENTIFY 应用命令参考

9.2.1. 选择命令

SELECT 命令用于选择 IDENTIFY 应用。

10.0.生命支持应用

这些产品的设计并非用于生命支持设备或系统，在这些设备或系统中对这些产品的误操作可能导致人身伤害。如果 ACS 客户将这些产品使用于或者销售用于此类应用，则他们应该自行承担相应的风险，而且同意赔偿由于不当使用或销售从而给 ACS 造成的损失。

11.0.联系方式

如需了解其他信息请访问 ACS 网站 http://www.acs.com.hk。

如需销售咨询请发送邮件至 info@acs.com.hk。