ICA

IoT合作伙伴计划联盟标准

ICA/T 2017-202-01

ID² 安全应用指令规范

Instruction specification of ID² application

2017－10－01 发布　　2017－10－01 实施

IoT 合作伙伴计划联盟发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由IoT合作伙伴计划联盟提出并归口。

本标准起草单位：阿里巴巴（中国）有限责任公司、北京智慧云测科技有限公司、北京同方微电子有限公司、北京握奇数据股份有限公司、Fingerprint Cards AB （FPC）、深圳市纽创信安科技开发有限公司、北京中电华大电子设计有限责任公司、捷德（中国）信息科技有限公司、国民技术股份有限公司、恩智浦（中国）管理有限公司、北京宝兴达信息技术有限公司、杭州晟元数据安全技术股份有限公司、金雅拓（北京）智能卡科技有限公司、苏州迈瑞微电子有限公司。

本标准主要起草人：马俊国、方强、安涛、黄天宁、葛风涛、王庆林、杨帆、张权、臧宏伟、孙婉丽、杨志雄、吴莹强、樊俊锋、闵晓宇、朱凯、于克兵、李毅、包乌日吐、张辉、陈肖琪、夏卓卿、赵永刚、谢懿、王慧、吕晨俊、许世波、赵荣霞、夏军虎、钱志恒、冯欢，牛建宾、李扬渊、卞维军、黄鑫。

本标准于2017年10月首次发布，本次为首次发布。

ID² 安全应用指令规范

1 范围

本标准规定了ID²安全应用安全报文、命令与应答、应用命令。

本标准适用于IoT合作伙伴计划联盟内采用 ID²进行物联网设备身份认证的安全可信应用。

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。

[1]《中国金融集成电路(IC)卡规范》 V3.0

[2]ISO/IEC 7816 PART 3：识别卡，带触点的集成电路卡：电气特性和传输协议。

[3]ISO/IEC 7816 PART 4：识别卡，带触点的集成电路卡：行业间交换用命令。

[4]GPC_Specification-2.2.1.10。

3 术语与定义

3.1 命令 command

终端向IC卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.2 响应 response

IC卡处理完成收到的命令报文后，返回给终端的报文。

3.3 功能 function

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

3.4 报文 Message

由终端向卡或卡向终端发出的，不含传输控制字符的字节串。

3.5 报文鉴别代码 Message Authentication Code

对交易数据及其相关参数进行运算后产生的代码。主要用于验证报文的完整性。

3.6 明文 Plaintext

没有加密的信息。

3.7 密文 Ciphertext

通过密码系统产生的不可理解的文字或信号。

3.8 密钥 Key

控制加密转换操作的符号序列。

3.9 保密密钥 Secret Key

对称加密技术中仅供指定实体所用的密钥。

3.10 加密算法 Cryptographic Algorithm

为了隐藏或揭露信息内容而变换数据的算法。

3.11 对称加密技术 Symmetric Cryptographic Technique

发送方和接收方使用相同保密密钥进行数据变换的加密技术。在不掌握保密密钥的情况下，不可能推导出发送方或接收方的数据变换。

3.12 数据完整性 Data Integrity

数据不受未经许可的方法变更或破坏的属性。

3.13 非对称加密技术 Asymmetric Cryptographic Technique

采用两种相关变换进行加密的技术，一种是公开变换（由公共密钥定义），另一种是私有变换（由私有密钥定义）。这两种变换具有以下属性，即私有变换不能通过给定的公开变换导出。

3.14 认证机构 Certification Authority

利用公开密钥和其他相关数据为所有者提供可靠校验的第三方机构。

3.15 数字签名 Digital Signature

一种非对称加密数据变换，它使得接受方能够验证数据的原始性和完整性，保护发送和接受的数据不被第三方伪造，同时对于发送方来说，还可用以防止接收方的伪造。

3.16 公开密钥认证 Public Key Certification

由认证机构签发的一个实体的公共密钥信息，具有不可伪造性。

3.17 私有密钥 Private Key

一个实体的非对称密钥对中仅供实体自身使用的密钥,在数字签名模式中,私有密钥用于签名功能。

3.18 公共密钥 Public Key

一个实体的非对称密钥对中可以公开的密钥，在数字签名模式中，公共密钥用于验证功能。

4 缩略语

下列缩略语适用于本文件。

AID 应用标识符（Application Identifier）
APDU 应用协议数据单元（Application Protocol Data Unit）
ATR 复位应答（Answer to Reset）
b 二进制（Binary）
BER 基本编码规则（Basic Encoding Rules）

BWI 块等待时间整数（Block Waiting Time Integer）
CLA 命令报文的类别字节（Class Byte of the Command Message）
CWI 字符等待时间整数（Character Waiting Time Integer）
DEA 数据加密算法（Data Encryption Algorithm）
DES 数据加密标准（Data Encryption Standard）
DF 专用文件（Dedicated File）
EDC 错误检测代码（Error Detection Code）
EF 基本文件（Elementary File）
Etu 基本时间单元（Elementary Time Unit）
FCI 文件控制信息（File Control Information）
FID 文件标识（File Identifier）
GND 地（Ground）
Hex. 十六进制数（Hexadecimal）
IC 集成电路（Integrated Circuit）
ICC 集成电路卡（Integrated Circuit Card）
IEC 国际电工委员会（International Electrotechnical Commission）
INS 命令的指令字节（Instruction Byte of Command Message）
ISO 国际标准化组织（International Standardization Organization）
Lc 终端发出的命令数据域的实际长度
Le 响应数据的最大期望长度
LEN 长度（Length）
MAC 报文鉴别代码（Message Authentication Code）
MF 主控文件（Master File）
P1 参数 1（Parameter 1）
P2 参数 2（Parameter 2）
PBOC 中国人民银行
PIN 个人密码（Personal Identification Number）
PIX 专用应用标识符扩展码（Proprietary Application Identifier Extension）
PSA 支付系统应用（Payment System Application）
PSAM 消费安全存取模块（Purchase Secure Access Module）
PSE 支付系统环境（Payment System Environment）
RFU 保留为将来使用（Reserved for Future Use）
RID 已注册的应用提供者标识（Registered Application Provider Identify）
RSA 一种非对称加密算法（Rivest,Shamir,Adleman）
RST 复位（Reset）
SAM 安全存取模块（Secure Access Module）
SFI 短文件标识符（Short File Identifier）
SHA 安全哈什算法（Secure Hash Algorithm）
SW1 状态码 1（Status Word One）
SW2 状态码 2（Status Word Two）

5 ID² 安全应用概述

5.1 ID² 定义

ID²（Internet Device ID）为内含设备唯一标识、对应密钥、证书、以及 ID² Server 的公钥字符串，其固化在芯片中，不可篡改、不可预测、全球唯一。

5.2 ID² 功能

根据作用对象不同，ID²具备以下功能。

- 设备端：ID²可作为信任锚完成设备身份认证或衍生会话密钥等；
- 云端：ID²可提供设备认证服务；
- 设备间：ID²可提供离线身份认证。

5.3 ID² 安全架构及特性

ID² 架构图如下：

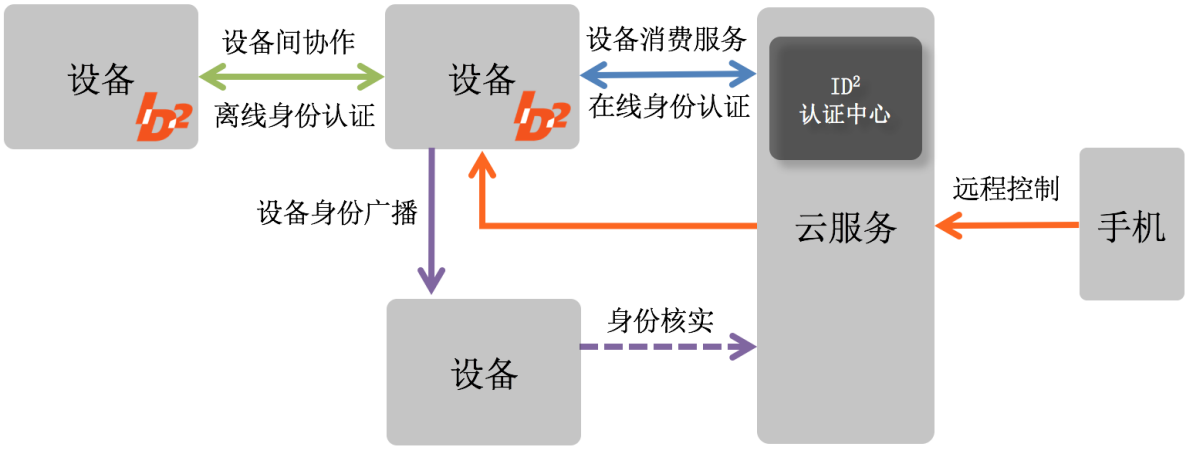

图1 ID²架构图

ID² 安全应用符合ISO7816和PBOC标准，满足IoT合作伙伴计划联盟内物联网设备身份识别认证需求的高安全可信应用。

ID² 安全应用安全特性图如下：

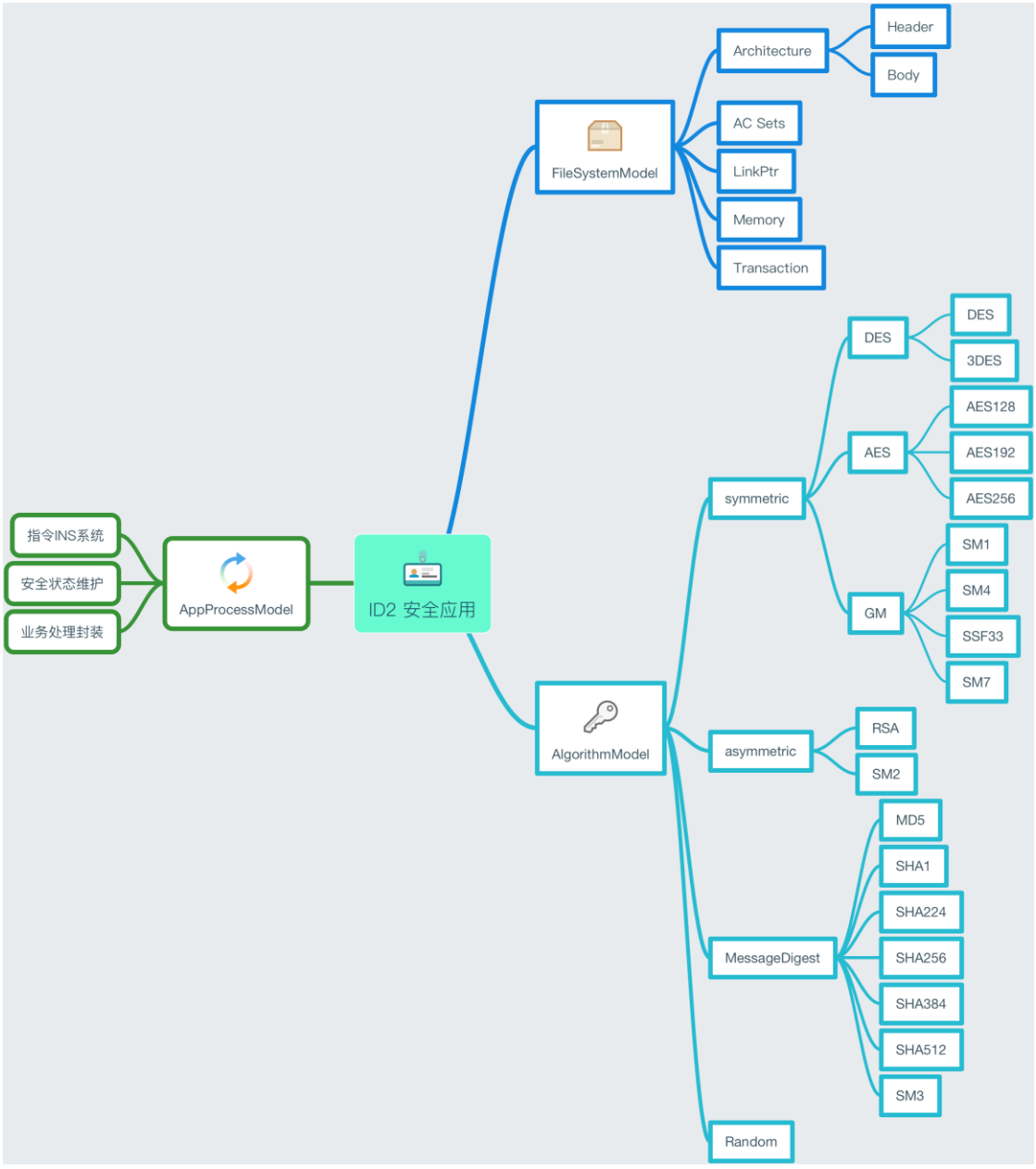

图2 ID²安全应用安全特性

ID² 安全应用安全特性如下：

- 支持 MD5/HASH（SHA1/224/256/512）/SM3 等主流摘要算法，能快速完成摘要计算。
- 支持 DES / AES / SM4 等主流对称算法，能快速完成加解密，MAC 运算及认证。
- 支持 RSA/SM2 非对称加密算法，能够快速完成 RSA 算法的签名、签名认证。
- 支持 RSA/SM2 密钥对 applet 内生成。
- 支持动态创建文件组织形式。
- 在通讯过程中支持 GP 安全通道保护机制。
- 支持多种安全访问方式和权限（安全通道保护和口令保护）。

注：ID² 的算法支持程度可以参见《IoT安全芯片（SE）准入规范》，根据设备具体需求选择。

5.4 ID² 安全应用 AID

AID 设置如下[1]：

‘AliYun.ID²’：

0xA0, 0x00, 0x00, 0x00, 0x41, 0x6C, 0x69, 0x59, 0x75, 0x6E, 0x2E, 0x49, 0x44, 0x32

注[1]:本 AID 由 IoT 合作伙伴计划联盟暂定。

5.5 ID² 安全应用指令集

ID² 安全应用指令集如表 1 所示：

表 1 ID² 安全应用指令集

编号	指令名称	CLA	INS	功能描述	兼容性
1	ID²_GetChallenge	00	84	取随机数	专有
2	ID²_SecurityStoreData	84	E2	安全通道下存储读写指令	专有
3	ID²_ComputeDigest	80	F0	计算摘要值（SHA1/SHA256/SHA512/SM3）	专有
4	ID²_GenerateKeyPair	80	F2	生成密钥对	专有
5	ID²_AsymmetricEncrypt	80	F4	非对称算法	专有
6	ID²_SymmtricEncrypt	80	F6	对称算法（3DES / AES / SM）	专有
7	ID²_GetID	80	F8	获取 ID².ID 值	专有
8	ID²_GetVendorInfo	80	FC	获取厂商信息	专有

5.6 ID² 安全应用密钥存储标识定义如下：

密钥类型说明如表 2 所示：

表 2 ID² 安全应用支持的应用密钥说明

密钥类型	值	说明
3DES	‘00 ‘	Triple-DES 密钥类型，对称算法
AES	‘01 ‘	AES 密钥类型，对称算法
RSA_Standard	‘02’	RSA 标准密钥类型，非对称算法
RSA_CRT	‘03’	RSA 中国余数定理类型，非对称算法
SM2	‘04’	国密椭圆 SM2 算法，非对称算法
SM4	‘05’	国密 SM4 密钥类型，对称算法
SSF33	‘06’	SSF33 密钥类型，对称算法
SM7	‘07’	SM7 密钥类型，对称算法
SM9	‘08’	国密 SM9 密钥类型，非对称算法
SM1	‘09’	国密 SM1 密钥类型，对称算法
ECC	0A	ECC 密钥类型，非对称算法

密钥元素标识如表 3 所示：

表 3 ID² 安全应用密钥存储标识定义

类型	标志	长度（字节）	值
3DES	‘40’	‘10’ or ‘18’	密钥值
AES	‘41’	‘10’ or ‘18’ or ‘20’	密钥值

SM4	‘42’	‘10’	密钥值
SSF33	‘43’	‘10’	密钥值
SM7	‘44’	‘10’	密钥值
SM9	‘45’	‘20’	密钥值
SM1	‘46’	‘10’	密钥值
RSA-CRT-INVQ	‘49’	密钥模数长度 / 2	INVQ 值
RSA-CRT-DP	‘50’	密钥模数长度 / 2	DP 值
RSA-CRT-DQ	‘51’	密钥模数长度 / 2	DQ 值
SM2-W-X	‘60’	‘20’	公钥 W 的 X 值
SM2-W-Y	‘61’	‘20’	公钥 W 的 Y 值
SM2-S	‘62’	‘20’	私钥 S 值
RSA-D	‘64’	私钥值长度	私钥值
RSA-E	‘65’	‘04’	公钥指数值
RSA-N	‘6E’	公钥值长度	公钥模数值
RSA-CRT-P	‘70’	密钥模数长度 / 2	素数 P 值
RSA-CRT-Q	‘71’	密钥模数长度 / 2	素数 Q 值
ECC-W-X	‘72’	‘20’	公钥 W 的 X 值
ECC-W-Y	‘73’	‘20’	公钥 W 的 Y 值
ECC-S	74	‘20’	私钥 S 值

5.7 ID²的配置选项

ID²的 i 参数，通过 4 字节 bitmap 的形式定义了 ID²安全应用支持的功能。

B3 RFU。 B0 定义如下：（byte 0）

表 4 ID²配置选项 B0

b8	b7	b6	b5	b4	b3	b2	b1	描述
							1	支持 3DES 算法
						1		支持 AES 算法
					1			支持 SM4 算法
				1				支持 SM7 算法
x	x	x	x					RFU

B1 定义如下：（byte1）

表 5 ID² 配置选项 B1

b8	b7	b6	b5	b4	b3	b2	b1	描述
							1	支持 RSA 算法
						1		支持 RSA CRT 算法
					1			支持 SM2 算法
				1				支持 SM9 算法
			1					ECC
x	x	x						RFU

B2 定义如下：

(byte2)

表 6 ID² 配置选项 B2

b8	b7	b6	b5	b4	b3	b2	b1	描述
							1	支持 SHA-1 算法
						1		支持 SHA-224 算法
					1			支持 SHA-256 算法
				1				支持 SHA-384 算法
			1					支持 SHA-512 算法
		1						支持 SM3 算法
x	x							RFU

ID²安全应用默认支持 Initialize Update、External Authenticate。如：

- i = 0x010101，支持 3DES、RSA、SHA1 算法。
- i = 0x000001，支持 3DES 算法、不支持非对称算法。

6 ID² 安全应用安全报文

6.1 安全报文传送概述

安全报文传送的目的是保证数据的机密性、完整性和对发送方的认证。数据的机密性通过对数据域的加密来得到保证。数据完整性和对发送方的认证通过使用报文鉴别代码 MAC 来实现。

6.2 完整性保护

对传输的数据附加 4 字节 MAC 码，接收方收到后首先进行校验，校验正确的数据予以接受，防止对传输数据的篡改。

数据完整性和对发送方的认证通过使用 MAC 来实现。

6.3 机密性保护

对传输的数据进行 DES 加密。

数据的机密性通过对数据域的加密来得到保证。

6.4 机密性和完整性保护

对传输的数据进行对称加密，后对传输的数据附加 4 字节 MAC 码，接收方收到后首先进行校验，校验正确的数据予以接受。

采取何种方法进行安全报文传送由用户根据实际情况来决定。

6.5 安全报文传送

安全报文的传输是采用了 GP 2.2.2 的 SCP02/03 的模式，详细内容请参加《GPC Specification 2.2.1》。

7 命令与应答

7.1 命令与响应格式

从终端发出的命令和卡片响应的信息必须遵从以下 4 种格式。

a) **情形 1:**

命令 :	**CLA**	**INS**	**P1**	**P2**	**00**
响应 :	**SW1**	**SW2**			

b) **情形 2：**

命令:	CLA	INS	P1	P2	Le
响应:	Le 字节的 DATA			SW1	SW2

c) **情形 3：**

命令:	CLA	INS	P1	P2	Lc	DATA
响应 :	SW1	SW2				

d) **情形 4：**

命令:	CLA	INS	P1	P2	Lc	DATA	Le
响应:	Le 字节的 DATA				SW1	SW2	

7.2 命令格式

ID² Applet 命令由 4 字节的命令头和命令体组成，见表 7。

表 7 命令格式

命令头				**命令体**		
CLA	INS	P1	P2	Lc	DATA	Le

7.2.1 命令头域

命令头定义板报文的内容如下表 8 所示：

表 8 命令头域

代码	长度 (byte)	值 (Hex)	描述
CLA	1	X0	不带安全报文的命令
		X4	带安全报文的命令

INS	1	XX	指令代码
P1	1	XX	参数 1
P2	1	XX	参数 2

7.2.2 命令体

命令体中各项是可选的。

表 9 命令体域

代码	描述
Lc	命令数据域中 DATA 的长度，不带安全报文时该长度不可超过 255 字节， 带安全报文时该长度不超过 239 字节
Data	命令和响应中的数据域
Le	响应数据域中期望数据的长度。 Le=00，表示需要最大字节数。 不带安全报文时该长度不可超过 255 字节； 带安全报文时该长度不超过 239 字节。

7.3 响应数据格式

ID² Applet 命令的应答由数据和状态字组成，即 Data+SW 组成，见表 10。

表 10 响应数据格式

数据	状态字	
响应中接收的数据位串	SW1	SW2

7.4 返回数据

7.4.1 返回状态字（SW1SW2）

SW1 SW2 是卡片执行命令的返回代码，任何命令的返回信息都至少由一个状态字组成。返回数据域是可选项。

7.4.2 状态字 SW1SW2 意义

状态字表示命令处理的情况，即命令是否被正确执行、未被正确执行状态及原因。

状态字由 2 部分组成：

a) SW1（status word1）：表示命令处理状态；

b) SW2（status word1）：表示命令处理限定。

状态字描述如表 11 所示：

表 11 状态字

SW1	SW2	描述
90	00	正确执行
61	xx	ISO7816 T0 协议期望返回数据长度
62	81	回送的数据可能错误
62	83	选择文件无效，文件或密钥校验错误

63	Cx	X 表示还可再试次数
63	10	尚有数据未返回
64	00	状态标志未改变
65	81	写 EEPROM 不成功
67	00	错误的长度
69	00	CLA 与线路保护要求不匹配
69	01	无效的状态
69	81	命令与文件结构不相容
69	82	安全条件不满足
69	83	密钥被锁死
69	84	没有取随机数
69	85	使用条件不满足
69	86	没有选择当前可操作的文件
69	87	无安全报文
69	88	安全报文数据项不正确
6A	80	数据结构不正确/验签失败
6A	81	功能不支持
6A	82	文件未找到
6A	83	记录未找到
6A	84	空间不足
6A	86	参数 P1 P2 错误
6B	00	在达到 Le/Lc 字节之前文件结束，偏移量错误
6C	xx	Le 错误
6D	00	不支持的指令代码
6E	00	无效的 CLA
6E	01	命令顺序无效
6E	02	无安全环境或安全环境无效
6F	00	数据无效
93	03	应用已被锁定
94	01	算法不支持
94	02	密钥类型不支持
94	03	密钥未找到
94	04	ID 已经写入
94	05	该类型密钥已经存在
94	06	所需的 MAC 不可用
95	xx	XX 代表还有多少字节需要传输

注：

- 当 SW1 的高半字节为‘9’，且低半字节不为‘0’时，其含义依赖于相关应用。
- 当 SW1 的高半字节为‘6’，且低半字节不为‘0’时，其含义与应用无关。

8 ID² 安全应用命令

8.1 GetChallenge（取随机数）命令

8.1.1 定义和范围

Get Challenge命令用于向卡片请求一个用于安全过程的随机数。

该随机数只能用于紧随其后的下一条指令，无论下一条命令是否使用了该随机数，该随机数都将立即失效。

8.1.2 命令报文

命令报文如表12所示：

表 12 命令报文

代码	值
CLA	00
INS	84
P1	00
P2	00
Lc	不存在–
Data	不存在
Le	‘04’～‘10’

8.1.3 命令报文数据域

命令报文数据域不存在。

8.1.4 响应报文数据域

响应报文数据域为期望返回的随机数数据。

8.1.5 响应报文状态码

此命令执行成功的状态码为’9000’。
eSE 可能回送的警告状态码见 7.4.2 章节说明。

8.2 ID²_Compute Digest（计算摘要）命令

8.2.1 定义和范围

Compute Digest 命令是将命令输入的数据通过指定的摘要算法计算成一个摘要值。待计算的数据通过一条或多条计算摘要命令发送至 eSE，eSE 收完所有的待计算数据块后，返回一个固定长度的摘要结果。

8.2.2 命令报文

计算摘要命令报文如表13所示：

表 13 命令报文

代码	值
CLA	‘80’
INS	‘F0’
P1	块号（从0开始）
P2	01：表示最后一条数据； 00：表示非最后一条的级联数据
Lc	待处理数据的长度
Data	待处理数据
Le	不存在或者期望返回的散列值的长度

8.2.3 命令报文数据域

命令报文数据域包含待计算的数据。
格式定义：
P1=0：
命令报文数据域如表 14 所示：

表 14 命令报文数据

定义	字节数	说明
Type	1	摘要算法类型： 00：SHA1 01：SHA224 02：SHA256 03：SHA384 04：SHA512 05：SM3
Data	Lc- 1	待计算数据

P1 != ‘00’：

定义	字节数	说明
Data	Lc	待计算数据

8.2.4 响应报文数据域

若当前命令不是最后一条 HASH 计算命令，则响应报文不存在；
若当前命令是最后一条 HASH 计算命令，则响应报文为计算得到的散列值。

8.2.5 响应报文状态码

此命令执行成功的状态码为’9000’。
当 eSE 不支持数据域指定的摘要算法时，命令返回算法不支持的状态字（具体见章节 7.4.1）。
eSE 可能回送的警告状态码见 7.4.2 章节说明。

8.3 ID²_SecurityStorage（ 安全数据操作）命令

8.3.1 定义和范围

ID² _SecurityStorage命令用于读写ID² 存储在SE中的敏感数据。
敏感数据包括ID²的ID，ID²的密钥以及其他关联敏感数据。
该命令需要先进行内外部认证。

8.3.2 命令报文

ID² _SecurityStorage（ 安全数据操作）命令报文如表15所示：

表 15 命令报文

代码	值
CLA	84
INS	E2
P1	见P1参数说明
P2	见P2参数说明
Lc	数据域长度
Data	ID² 个人化数据
Le	不存在

P1 作为读写及块号控制参数，说明如下：
P1 最高位 Bit7 定义：

Bit7	说明
1	读指令
0	写指令

P1 次高位 Bit6 定义：

Bit6	说明
1	业务数据指令
0	密钥操作指令

P1 Bit5~Bit0 定义：

Bit5~Bit0	说明
‘XX’	表示级联数据的块号 取值范围：’00’~’20’

P2 参数表示级联标识，定义如下：

值	说明
‘01’	最后一条待处理数据
‘00’	表示级联待处理数据

8.3.3 命令报文数据域

当 P1-Bit7 = 0 时，表示写指令：
命令报文数据域包含待写入的数据格式定义如下：
a) 当数据域为密钥时,密钥头数据格式：

定义	字节数	说明
ID²_id 长度	‘1’	
ID²_id	X	ID²_ID的数据
KEY_TYPE	1	见表2
KEY_ID	1	‘00’：表示ID².Key密钥 ‘01’~‘FF’：表示业务关联密钥
KEY	见下表	

KEY 字段格式定义如下：

定义	字节数	说明
KeyEl01 Tag	1	第 1 个密钥元素的的 Tag，见 5.5 章节 密钥元素标识表
KeyEl01 Length	2	第 1 个密钥元素的长度
KeyEl01 Value	KeyEl Length	第 1 个密钥元素值
KeyEl02 Tag	1	第 2 个密钥元素的的 Tag，见 5.5 章节 密钥元素标识表
KeyEl02 Length	2	第 2 个密钥元素的长度
KeyEl02 Value	KeyEl Length	第 2 个密钥元素值
…		
KeyEln Tag	1	第 n 个密钥元素的的 Tag，见 5.5 章节 密钥元素标识表
KeyEln Length	2	第 n 个密钥元素的长度
KeyEln Value	KeyEl Length	第 n 个密钥元素值

注：

[1]装载 ID² 密钥数据为级联时，第一块数据为密钥头数据和第一包密钥值内容，后续块仅为密钥值内容;

[2]当密钥头数据长度+密钥数据值内容长度小于 256 字节长度时，必须一次性装载完所有密钥数据;

[3]KeyEl01~KeyEln 必须为同一密钥的密钥组成元素。

b) 当写入的数据为非密钥的业务类数据时，

定义	字节数	说明
Data	Lc	业务数据

注：

[1]读指令数据域不存在;

[2]密钥相关的业务关联设置及数据都放在业务数据中，由业务方与 OEM 厂商沟通确定。(如密钥尝试次数限制，密钥的管理维护权限等，ID²的密钥除外。)

8.3.4 响应报文数据域

当指令为写模式时，响应报文数据不存在。

当指令为读模式时，响应报文数据为业务关联数据。

注：不允许通过读指令读取密钥数据。

8.3.5 响应报文状态码

此命令执行成功的状态码为’9000’。

eSE 可能回送的警告状态码见 7.4.2 章节说明。

8.4 ID²_Generate KeyPair(生成密钥对)命令

8.4.1 定义和范围

Generate Key命令用于产生一个完整的非对称密钥公私钥对，公私钥将存储在相应的密钥文件中，具体的密钥记录由数据域指定的KID决定。产生的密钥对的公钥值，在响应报文中返回。

产生的密钥长度由命令数据域指定，密钥长度要求在64~256字节范围内，且必须是8的整数倍；例如RSA2048长度为256字节，数据域值为0x0800。

公钥的 KID 和私钥的 KID 必须保持一致。

注：

私钥 KID = 公钥 KID+0x01；

公钥头与私钥头的格式由厂商自行定义；

8.4.2 命令报文

ID²_Generate KeyPair(生成密钥对)命令报文如表16所示：

表 15 命令报文

代码	值
CLA	‘80’
INS	‘F2’
P1	见 P1 参数说明
P2	‘00’
Lc	‘04’
Data	见定义
Le	00

该指令必须在安全通道建立之后发送。

P1参数定义：

值	说明
00	生成密钥对
01	当返回数据域大于 256 长度时，读取剩余的公钥值

8.4.3 命令报文数据域

命令报文数据域包含密钥类型，密钥 KID 及两字节的密钥长度，用于指定该命令产生的非对称公私钥对的长度

定义	字节数	说明
密钥类型	‘1’	见表 2 密钥类型说明
密钥 KID	‘1’	‘XX’，公钥的KID
密钥长度	‘2’	密钥的BIT长度

注：若数据域的 KID 在应用中已经存在，则生成密钥对失败，报错密钥已存在。

8.4.4 响应报文数据域

响应报文数据域包含产生的公钥模。

响应报文数据域公钥数据格式结构如表 17 所示：

表 17 响应报文数据域

类型	标志（T）	长度（L）	值（V）	标志（T）	长度（L）	值（V）
RSA	6E	00（256bytes）	公钥值 N	65	04	‘00010001’
SM2	60	20	公钥值 X	61	20	公钥值 Y

8.4.5 响应报文状态码

此命令执行成功的状态码为’9000’。

eSE 可能回送的警告状态码见 7.4.2 章节说明。

8.5 ID²_AsymmetricCrypt（非对称算法）命令

8.5.1 定义和范围

ID²_AsymmetricCrypt命令用于非对称算法使用密钥进行非对称运算，包括加解密和签名验签。

8.5.2 命令报文

ID²_AsymmetricCrypt（非对称算法）命令报文如表 18 所示：

表 18 命令报文

代码	值
CLA	80
INS	F4
P1	见 P1 参数说明
P2	‘01’：表示最后一条待处理数据； ‘00’：表示级联待处理数据
Lc	待处理数据长度 （当 P1=‘00’时，为待处理数据+5 字节数据头）

	或 不存在(当 P1=‘40’时，表示取剩余待返回数据，Lc 不存在)
Data	待处理数据
Le	‘00’/’XX’(当 P1=’40’时，表示读取剩余待返回数据)

P1 参数定义：

Bit7~Bit6	Bit5~Bit0	说明
0	-	应用指令
1	-	当返回数据域大于 256 长度时，读取剩余的返回值
	‘00’~‘20’	表示块号，‘00’为起始块号

8.5.3 命令报文数据域

命令报文数据域为待加密的数据，其内容要求如表 19 所示：

表 19 命令报文数据域

定义	字节数	说明	备注
模式	1	0x51:加密 0x52:解密 0x53:签名 0x54:验签	当 P1=‘00’时，该部分数据域存在
算法类型	1	00：RSA_NOPADDING 01：RSA_SHA1(RSA_PKCS1) 02:RSA_SHA256 03:RSA_SHA384 04:_RSA_SHA512 05：SM2_SM3 06:ECDSA	
KID	1	KEY 索引，‘00’~‘FF’	
Length	2	待处理数据长度	
Data	Length	待处理数据	-

注：数据域说明

P1	P2	模式	算法类型	Data	说明
00	00/01	0x51,0x52	00,01	1 字节 KID+ 2 字节长度+数据	P1P2：0001 表示仅有一块数据
		0x53,0x54	01,02,03, 04,05,06		
0x01-0x20		——	——	数据	第 n 块
0x40	00	——	——	--	Le:xx 剩余待返回数据长度

注：验签数据格式要求，验签明文数据+签名数据

8.5.4 响应报文数据域

响应报文数据域为加密的密文，其内容要求如表 20 所示：

表 20 响应报文数据域

定义	要求
响应数据总长度(2 字节)	在第一次响应中返回
RSA	密文长度=算法模长
SM2_SM3_	C1C3C2，其中 C1 长度为 32bytes C3 长度为 32bytes C2 长度最大不超过 256bytes

8.5.5 响应报文状态码

此命令执行成功的状态码为’9000’。
eSE 可能回送的警告状态码见 7.4.2 章节说明。

8.6 ID²_SymmetricCrypt（对称算法）命令

8.6.1 定义和范围

ID²_SymmetricCrypt 命令用于对称加密或 MAC 计算。

8.6.2 命令报文

ID²_SymmetricCrypt（对称算法）命令报文如表21所示：

表 21 命令报文

代码	值
CLA	80
INS	F6
P1	块号：‘00’~‘20’ ‘00’为起始块号
P2	‘01’：表示最后一条待处理数据； ‘00’：表示级联待处理数据
Lc	待处理数据长度
Data	待处理的数据
Le	不存在或期望返回数据的长度

8.6.3 命令报文数据域

命令报文数据域为待处理数据。

定义	字节数	说明
模式	1	0x51:加密操作 0x52:解密操作 0x53:计算 MAC 0x54:验证 MAC

算法类型	1	‘00’：DES_CBC_NOPADDING ‘01’：DES_ECB_NOPADDING ‘02’：AES_CBC_NOPADDING ‘03’：AES_ECB_NOPADDING ‘04’：DES_CBC_ISO9797_M1 ‘05’：DES_CBC_ISO9797_M2 ‘06’：AES_CBC_ISO9797_M1 ‘07’：AES_CBC_ISO9797_M2 ‘10’：SM4_CBC_NOPADDING ‘11’：SM4_ECB_NOPADDING ‘12’：SM7_CBC_NOPADDING ‘13’：SM7_ECB_NOPADDING ‘14’：SM4_CBC_ISO9797_M1 ‘15’：SM4_CBC_ISO9797_M2 ‘16’：SM7_CBC_ISO9797_M1 ‘17’：SM7_CBC_ISO9797_M2
KID	1	KEY 索引，‘00’～‘FF’
Length	2	待处理数据总长度
Data	Length	待处理数据

注：

[1] 完整的数据域说明如下，如完整数据长度超过一条命令的最大长度时，可根据情况拆分成多条级联命令处理。只有第一包存在算法模式+算法类型+KID;

[2] 对称算法的加解密 Padding 统一都设置为 Nopadding。所有运算数据的填充方式及填充动作均在 eSE 外部实体中完成后，再送入 eSE 进行密钥运算。

[3] 对称算法的 MAC 计算，除了支持 Nopadding 模式，同时也支持 M1 和 M2 的 Padding 格式。

[4]Data 域说明如下：

定义	模式	算法类型	字节数	说明
IV	‘0x51、‘0x52’、‘0x53’、‘0x54’	‘0x00’	8	初始向量
		‘0x02’、‘0x04’、‘0x05’、‘0x06’、‘0x07’、‘0x10’、‘0x12’、‘0x14’‘0x15’、‘0x16’、‘0x17’	16	
		其他	0	
数据	全部	全部		待计算数据
MAC	‘0x54’	‘0x00’	8	待验证 MAC
		‘0x02’、‘0x04’、‘0x05’、‘0x06’、‘0x07’、‘0x10’、‘0x12’、‘0x14’‘0x15’、‘0x16’、	16	

		‘0x17’		
	其他	全部	0	

8.6.4 响应报文数据域

响应报文数据域返回（对称算法结果数据或MAC值）。

计算结果说明如下：

模式	字节数	说明
‘0x51’:加密操作 ‘0x52’:解密操作	0或 8/16整数倍	当收到密钥算法块长度的数据后进行加解密运算并返回
‘0x53’:计算MAC	0或8/16	在收到所有数据后返回MAC值，MAC值为CBC算法计算的最后一块。
‘0x54’:验证MAC	0	无返回

MAC运算采用ISO-9797运算方法。

8.6.5 响应报文状态码

此命令执行成功的状态码为’9000’。

eSE可能回送的警告状态码见7.4.2章节说明。

8.7 ID²_GetID（获取ID²的ID值）命令

8.7.1 定义和范围

ID²_GetID命令用于从ID²安全应用中读取ID²的ID值。

8.7.2 命令报文

ID²_GetID（获取ID²的ID值）命令报文如表22所示：

代码	值
CLA	‘80’
INS	‘F8’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	‘XX’

8.7.3 命令报文数据域

命令报文数据域不存在。

8.7.4 响应报文数据域

响应报文数据域要求如下：

返回的数据是厂商的信息，其信息格式如下

信息	**字节数**	**说明**
厂商标识	2	-
Length	1	ID²的ID Length

ID² 的 ID 值	Length	ID² 的 ID 值字串

8.7.5 响应报文状态码

此命令执行成功的状态码为’9000’。
eSE 可能回送的警告状态码见 7.4.2 章节说明。

8.8 ID²_GetVendorInfo（获取厂商信息）命令

8.8.1 定义和范围

Get Vendor Info 命令用于向卡片请求厂商信息。

8.8.2 命令报文

代码	值
CLA	80
INS	FC
P1	00
P2	00
Lc	不存在
Data	不存在
Le	XX

8.8.3 命令报文数据域

命令报文数据域不存在。

8.8.4 响应报文数据域

响应报文数据域要求如下：
返回的数据是厂商的信息，其信息格式如下

信息	**长度**
厂商标识	2 字节
版本信息	8 字节
ID²配置选项	4 字节
可用空间	2 字节
扩展位	4 字节

8.8.5 响应报文状态码

此命令执行成功的状态码为’9000’。
eSE 可能回送的警告状态码见 7.4.2 章节说明。

8.9 ID²_Verify PIN（验证 PIN）命令（可选）

8.9.1 定义和范围

Verify PIN命令要求eSE中的应用验证外部输入的密码（PIN）。

执行该命令前，需先执行 Get Challenge 命令，获取 16 字节的随机数。

PIN 验证成功后，将获得相关的安全状态。

PIN 验证失败后，剩余尝试次数递减，相关的安全状态被清除，并返回 63Cx。若持续验证失败，剩余尝试次数将递减为 0，PIN 将被锁定；可以通过 Reload PIN 或 Unblock PIN 解锁。

8.9.2 命令报文

代码	值
CLA	00
INS	20
P1	00
P2	00
Lc	‘10’
Data	认证密文数据
Le	不存在

8.9.3 命令报文数据域

命令报文数据域包含认证密文数据。采用摘要算法对用户输入的密码(仅使用 PIN 的有效数据)进行计算，以摘要计算结果的高 16 字节作为密钥，对 Get Challenge 命令返回的随机数采用对称算法进行 ECB 加密计算，得到 PIN 认证的密文数据。

使用的摘要算法和对称算法由应用确定。

8.9.4 响应报文数据域

响应报文数据不存在。

8.9.5 响应报文状态码

此命令执行成功的状态码为’9000’。

eSE 可能回送的警告状态码见 7.4.2 章节说明。

8.10 ID²_Write／UpdatePIN（ 装载／更新 PIN ） 命令 （可选）

8.10.1 定义和范围

Write/UpdatePIN 命令用于装载/更新 PIN。

PIN 不存在时，只允许装载，不允许更新；PIN 已存在时，只允许更新，不允许装载。

该命令用于更新 PIN 时，命令数据域包含 PIN 认证密文数据和 PIN 密文值。执行该命令前，需要先执行 Get Challenge 命令，获取 16 字节的随机数。

8.10.2 命令报文

代码	值
CLA	84
INS	24
P1	00/01

	P1=‘00’ ： 表示装载PIN P1=’01’： 表示更新已有的PIN值，加密存储
P2	00
Lc	数据域长度
Data	P1=’00’时：PIN值 P1=‘01’：PIN认证密文数据和PIN密文值
Le	不存在

8.10.3 命令报文数据域

PIN 值为 BCD 编码，长度仅支持 8 字节和 16 字节两种情况。

如果 P1=‘00’，装载新 PIN，命令报文数据如下格式：

PIN 尝试次数上限	PIN 明文值(16 字节)
XX（‘01’～‘0F’）	实际 PIN 长度为 8 字节时，以 8 字节‘FF’右填充。

如果 P1=‘01’，更新已有的 PIN 值，命令报文数据域如下格式：

PIN 认证密文数据	PIN 密文值(16 字节)
与 ID²_Verify PIN 命令中的认证密文数据相同。 PIN 验证成功后，将获得相关的安全状态。 PIN 验证失败后，剩余尝试次数递减，相关的安全状态被清除，并返回 63Cx。若持续验证失败，剩余尝试次数将递减为 0，PIN 将被锁定；可以通过 Reload PIN 或 Unblock PIN 解锁。	使用计算PIN认证密文数据中所用的对称密钥对新 PIN 进行 CBC 加密，使用获取的 16 字节的随机数作为 ICV。 新 PIN 为 8 字节时，以 8 字节‘FF’右填充后再加密。

摘要算法和对称算法由应用确定。

对称算法选用遵从以下优先原则：

AES>DES>SM4>SM7>SM1

8.10.4 响应报文数据域

响应报文数据不存在。

8.10.5 响应报文状态码

此命令执行成功的状态码为’9000’。

eSE 可能回送的警告状态码见 7.4.2 章节说明。

8.11 ID²_Reload / Unblock PIN（ 重装 / 解锁 PIN ） 命令 （可选）

8.11.1 定义和范围

Reload/Unblock PIN 命令用于重装/解锁 PIN，命令使用特定的对称密钥计算 MAC。

Reload PIN 执行成功后，PIN 值更新，同时剩余尝试次数恢复为上限；Unblock PIN 执行成功后，仅 PIN 的剩余尝试次数恢复为上限。

MAC 验证错误时，对称密钥的剩余尝试次数递减；递减为 0 时，对称密钥锁定。(对称密钥的尝试

次数在装载密钥时进行设定。）

执行该命令前，需要先执行 Get Challenge 命令，获取 8/16 字节的随机数。

8.11.2 命令报文

代码	值
CLA	84
INS	5E
P1	00/01 P1=‘00’： 表示Reload PIN P1=’01’： 表示Unblock PIN
P2	00
Lc	数据域长度
Data	P1=‘00’：PIN密文+MAC P1=‘01’：MAC
Le	不存在

8.11.3 命令报文数据域

Reload PIN 命令的密文数据为对称密钥对新 PIN 值的 CBC 加密的结果，以随机数作为 ICV，PIN 长度为 8 字节时，以 8 字节‘FF’右填充。

MAC 通过对称密钥对命令头+可能的密文数据计算得到，已获取的 8/16 字节随机数作为 MAC 计算的 ICV，取计算结果的前 4 字节为 MAC。

对称密钥的 KID 由业务应用需求方制定，且 KID≠0x00。

8.11.4 响应报文数据域

响应报文数据不存在。

8.11.5 响应报文状态码

此命令执行成功的状态码为’9000’。

eSE 可能回送的警告状态码见 7.4.2 章节说明。

附录 A

（规范性附录）

厂商标识

A.1 厂商标识

IoT 合作伙伴计划联盟中厂商使用 ID²安全应用指令时标识如下:

安全厂商	厂商标识
金雅拓	8080
握奇数据	8081
捷德	8082
华大	8180
国民技术	8181
恩智浦	8182
同方微	8183
晟元	8184
英飞凌	8185
意法半导体	8186

注：新申请的安全厂商，其厂商标识由联盟统一分配。

附录 B

（规范性附录）

CMAC运算规则

B.1 .CMAC运算规则

算法过程具体可参照[ISO 9797-1]中规定的” MAC Algorithm 1”。