ICS 35.040
L 80

中华人民共和国国家标准

GB/T 33746.1—2017

近场通信(NFC)安全技术要求
第1部分:NFCIP-1安全服务和协议

Technical specification of NFC security—
Part 1: NFCIP-1 security services and protocol

(ISO/IEC 13157-1:2010, Information technology—Telecommunications and information exchange between systems—NFC Security—Part 1: NFC-SEC NFCIP-1 security services and protocol, MOD)

2017-09-07 发布　　2018-04-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 33746《近场通信(NFC)安全技术要求》分为以下 2 部分：

——第 1 部分：NFCIP-1 安全服务和协议；

——第 2 部分：安全机制要求。

本部分为 GB/T 33746 的第 1 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用重新起草法修改采用 ISO/IEC 13157-1：2010《信息技术　系统间通信及信息交互 NFC 安全　第 1 部分：NFC 安全 NFCIP-1 安全服务和协议》。

本部分与 ISO/IEC 13157-1：2010 的技术性差异及其原因如下：

——将原标准的规范性引用文件中的 ISO 标准更改为对应的国标；

——删除了两个国标中没有用到的术语 LSB 和 MSB；

——在第 7 章增加“本部分中涉及的密码算法应遵循国家商用密码的有关规定。”；

——为了避免悬置段的产生调整了 8、9、10、11 章的章节号；

——附录的顺序按照国标要求，原 ISO 标准的附录 A 和附录 B，按提及的先后顺序，分别变为本部分的附录 B 和附录 A。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：工业和信息化部电信研究院、西安西电捷通无线网络通信股份有限公司、中国普天信息产业股份有限公司、中国物品编码中心、国家射频识别产品质量监督检验中心。

本部分主要起草人：张琳琳、孙倩、杨军、杜志强、胡亚楠、朱锋、姜国强、鄢若韫、李卓凡、李志敏。

近场通信(NFC)安全技术要求
第1部分:NFCIP-1安全服务和协议

1 范围

GB/T 33746的本部分规定了NFCIP-1的NFC-SEC安全通道服务和共享秘密服务,以及相应服务使用的PDU和协议。

本部分适用于NFCIP-1安全服务和协议的要求。

注1:NFC-SEC专为ISO/IEC 18092中规定的数据交换协议而设计。

注2:本部分不提出与特定应用相关的安全机制(例如:ISO/IEC 7816系列标准中提出的智能卡应用案例需要的安全机制)。NFC-SEC可作为ISO/IEC 7816中应用安全机制的补充。

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。

GB/T 9387.1—1998 信息技术 开放系统互连 基本参考模型 第1部分:基本模型(ISO/IEC 7498-1:1994,IDT)

GB/T 17967—2000 信息技术 开放系统互连 基本参考模型 OSI服务定义约定(ISO/IEC 10731:1994,IDT)

GB/T 25069—2010 信息安全技术 术语

GB/T 33746.2—2017 近场通信(NFC)安全技术要求 第2部分:安全机制要求(ISO/IEC 13157-2:2010,MOD)

ISO/IEC 18092:2004 信息技术 系统间远程通信和信息交换 近场通信 接口和协议 NFCIP-1 [Information technology—Telecommunications and information exchange between systems—Near Field Communication—Interface and Protocol (NFCIP-1)]

3 术语和定义

GB/T 17967—2000、GB/T 25069—2010和ISO/IEC 18092:2004界定的以及下列术语和定义适用于本文件。

3.1

连接密钥 link key

保证安全通道安全性的密钥。

3.2

NFC-SEC用户 NFC-SEC user

使用NFC-SEC服务的实体。

3.3

接收者 recipient

接收ACT-REQ命令的NFC-SEC实体。

3.4

安全通道　secure channel

安全的 NFC-SEC 连接。

3.5

发送者　sender

发送 ACT-REQ 命令的 NFC-SEC 实体。

3.6

共享秘密　shared secret

对等 NFC-SEC 用户间所共享的秘密。

4　数字表示形式和符号

下列数字表示形式和符号均适用于本文件。

4.1　数字表示形式

数字表示形式如下所示：

- 括号内的字母和数字表示十六进制数。
- 比特位设置为 0 或 1。
- 二进制数和比特位模式均表示为 0 和 1 的序列且最高有效位在左侧。在数据串中，X 可表示该位数据在数据串没有被明确设置。
- 在 8 位字节中最低有效位是比特 0，最高有效位是比特 7。

4.2　符号

基本元素的名称，例如：特定字段，均表示为对应英文单词的首字母大写。

5　缩略语

下列缩略语适用于本文件。

ACT_REQ	激活请求 PDU	(Activation Request PDU)
ACT_RES	激活响应 PDU	(Activation Response PDU)
ATR_REQ	属性请求	(Attribute Request)
ATR_RES	属性响应	(Attribute Response)
DEP	数据交换协议请求及数据交换协议响应	(Data Exchange Protocol Request and Data Exchange Protocol Response)
DID	设备 ID	(Device ID)
ENC	加密包 PDU	(Encrypted Packet PDU)
ERROR	错误 PDU	(Error PDU)
lsb	最低有效位	(least significant bit)
MI	数据交换协议的多信息链接	(Multiple Information link for Data Exchange Protocol)

msb	最高有效位	(most significant bit)
MSG	消息码	(MesSaGe code)
NAD	节点地址	(Node Address)
NFCIP-1	近场通信-接口和协议-1	(Near Field Communication-Interface and Protocol-1)
NFC-SEC	近场通信-安全	(Near Field Communication-Security)
PCI	协议控制信息	(Protocol Control Information)
PDU	协议数据单元	(Protocol Data Unit)
PFB	交易控制信息	(Control Information for Transaction)
PID	协议标识符	(Protocol Identifier)
PNI	包编号信息	(Packet Number Information)
PPi	初始方使用的协议参数	(Protocol Parameters used by Initiator)
PPt	目标方使用的协议参数	(Protocol Parameters used by Target)
RFU	预留位	(Reserved for Future Use)
SAP	服务访问点	(Service Access Point)
SCH	安全通道服务	(Secure Channel service)
SDL	规范和说明语言	(Specification and Description Language)
SDU	服务数据单元	(Service Data Unit)
SEP	安全交换协议参数	(Security Exchange protocol Parameter)
SN	序列号	(Sequence Number)
SNV	序列号变量	(SN variable)
SSE	共享秘密服务	(Shared Secret Service)
SVC	服务代码	(SerVice code)
TMN_	终止 PDU	(Terminate PDU)
VFY_REQ	验证请求 PDU	(Verification Request PDU)
VFY_RES	验证响应 PDU	(Verification Response PDU)

6 符合性

声称符合本部分规定的一个或多个安全服务的实现应采用由选定的 PID 对应的 NFC-SEC 密码部分的安全机制。

使用 NFCIP-1 协议的实现在声称符合本部分时还应满足附录 A 的要求。

7 概要

图 1 的 NFC-SEC 使用了 GB/T 9387.1—1998 中定义的 OSI 参考模型。

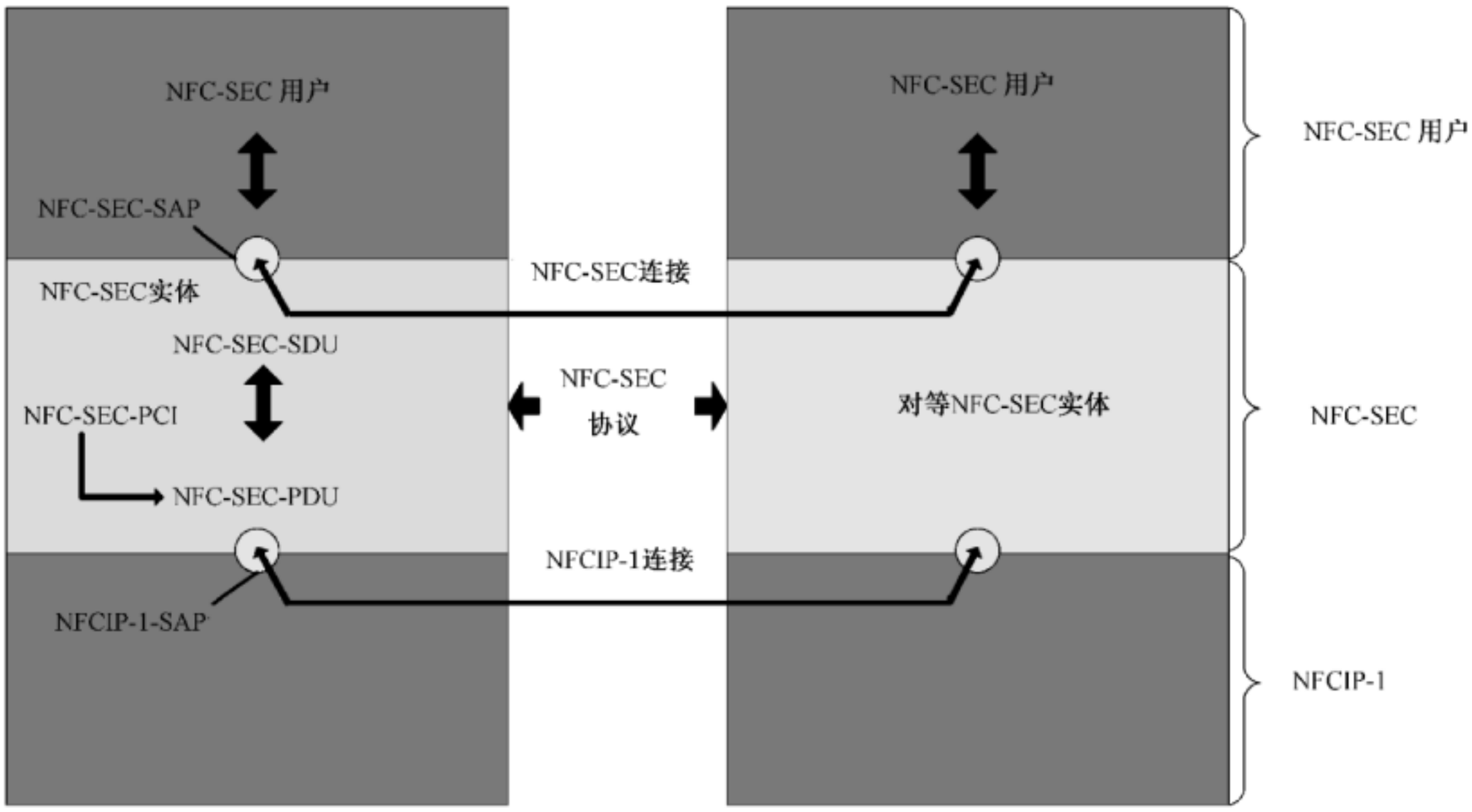

图 1　NFC-SEC 架构

NFC-SEC 用户通过 NFC-SEC 服务访问点(NFC-SEC-SAP)来激活和访问 NFC-SEC 服务。NFC-SEC 实体从 NFC-SEC 用户处获取 NFC-SEC-SDU (请求)并且向 NFC-SEC 用户返回 NFC-SEC-SDU (确认)。

本部分规定了安全通道服务(SCH)和共享秘密服务(SSE)。本部分中涉及的密码算法应遵循国家商用密码的有关规定。

为提供 NFC-SEC 服务,对等 NFC-SEC 实体根据 NFC-SEC 协议要求,在 NFC-SEC 连接上交换 NFC-SEC-PDU。

对等 NFC-SEC 实体之间通过 NFCIP-1 服务访问点(NFCIP-1-SAP)来互相通信,访问 NFCIP-1 数据服务,发送和接收 NFC-SEC-PDU。一个 NFC-SEC-PDU 包含 NFC-SEC 协议控制信息(NFC-SEC-PCI)和一个单独的 NFC-SEC-SDU。

8　服务

8.1　概述

本章规定了 NFC-SEC 向 NFC-SEC 用户提供的两种服务:SSE 和 SCH。一旦服务被调用,这些服务将采用第 9 章定义的协议以密码方式保护对等实体间 NFC-SEC 用户消息的传输。

下面介绍的共享秘密的建立应与任何之前或之后建立的共享秘密没有加密相关性。

8.2　共享秘密服务(SSE)

SSE 在两个对等用户之间建立一个共享秘密,用户可自行使用。

调用 SSE 应根据 GB/T 33746.2—2017 提供的密钥协商和密钥确认机制建立共享秘密。

8.3　安全通道服务(SCH)

SCH 提供一个安全通道。

调用 SCH 应根据 GB/T 33746.2—2017 提供的方法,通过密钥协商和密钥确认机制建立的共享秘

密来导出连接密钥，并且应保护之后通道中的双向通信安全。

9 协议机制

9.1 流程

NFC-SEC 协议包含以下机制。图 2 展示了协议机制流程。

9.2 密钥协商

根据 GB/T 33746.2—2017 提供的方法，对等 NFC-SEC 实体应使用 ACT_REQ 和 ACT_RES 来建立共享秘密。

9.3 密钥确认

根据 GB/T 33746.2—2017 提供的方法，对等 NFC-SEC 实体应使用 VFY_REQ 和 VFY_RES 来确认共享秘密。

9.4 PDU 安全

PDU 安全只是 SCH 服务中的一种机制。

对等的 NFC-SEC 实体应根据 GB/T 33746.2—2017 提供的方法，使用 ENC 保护数据交换。

根据相应的 GB/T 33746.2—2017 中的定义，本机制应包含下列中的一项或几项：

——序列完整性，与 12.3 的要求一致；

——机密性；

——数据完整性；

——原发鉴别。

9.5 终止

对等 NFC-SEC 实体间应使用 TMN 来终止 SSE 和 SCH。当 NFCIP-1 协议被释放或者取消，或者 NFCIP-1 设备电源关闭时，应终止 SSE 和 SCH 实例。当转变为空闲(IDLE)状态时，应销毁相应的共享秘密和连接密钥。

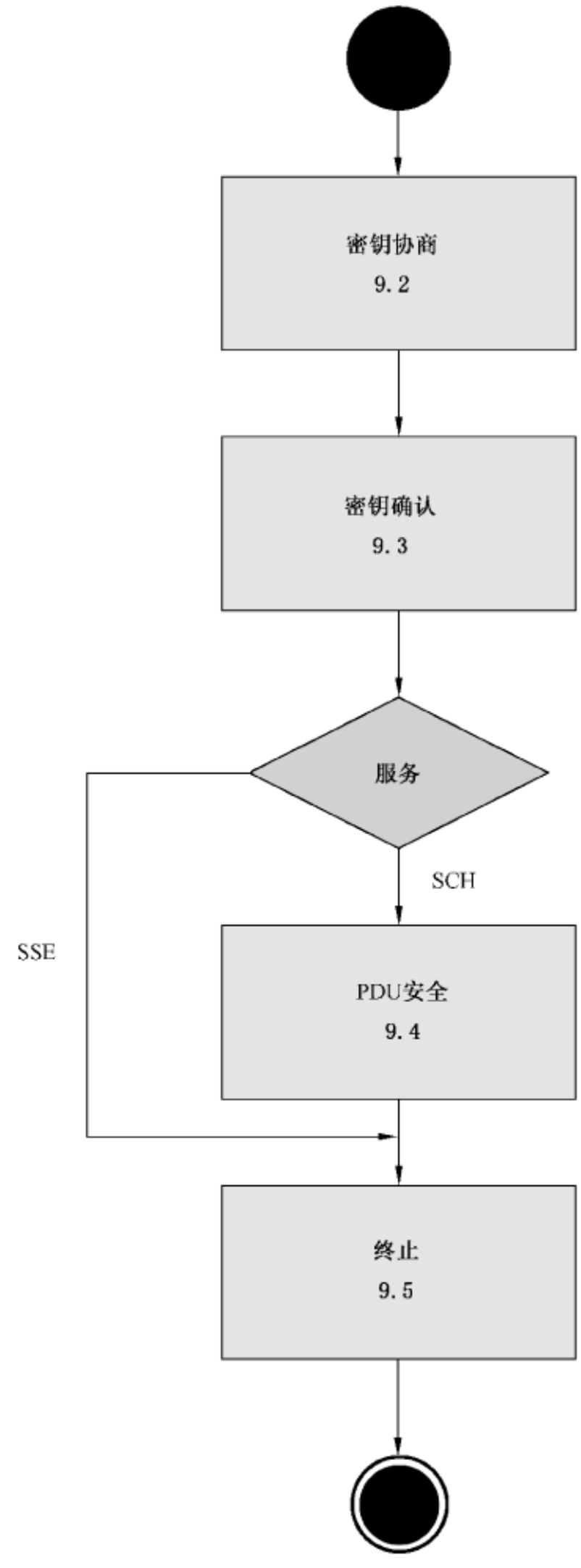

图 2　NFC-SEC 服务常规流程

10　状态和子状态

附录 B 中的 NFC-SEC 协议机规定了表 1 中状态和子状态之间的转换。

表 1　状态

状态	描述
空闲(Idle)	NFC-SEC 准备通过向 NFC-SEC 用户或者其对等实体发送请求来启动新服务
选择(Select)	NFC-SEC 正在等待 ACT_RES
建立(Established)	请求 NFC-SEC 服务。“建立”状态包含两个子状态,“建立_发送者”(“Established_Sender”)子状态等待 VFY_RES,“建立_接收者”(“Established_Recipient”)子状态等待 VFY_REQ
确认(Confirmed)	已建立一个 NFC_SEC 服务。“确认”状态包含两个子状态,在“确认_SSE”(“Confirmed_SSE”)子状态中取出共享秘密,在“确认_SCH”(“Confirmed_SCH”)子状态中,准备开始安全数据传输

11　NFC-SEC-PDU

11.1　结构

NFC-SEC-PDU 应在 NFCIP-1 DEP(数据交换协议请求及数据交换协议响应)“安全数据”PDU 中传送,并把 DEP 传输数据中的 SEP 字节作为第 0 个字节。DEP 传输数据应只包含一个 NFC-SEC-PDU。

NFC-SEC-PDU 结构见图 3。

SEP	PID	NFC-SEC 有效载荷

图 3　NFC-SEC-PDU 结构

表 2 把 NFC-SEC-PDU 的字段分为 3 种类型:必选(m),禁止(p)和可选(c)。可选字段将在 11.4 中进一步说明。

表 2　NFC-SEC-PDU 字段

NFC-SEC-PDU	SEP	PID	NFC-SEC 有效载荷
ACT_REQ	m	m	c
ACT_RES	m	p	c
VFY_REQ	m	p	c
VFY_RES	m	p	c
ENC	m	p	c
TMN	m	p	p
ERROR	m	p	c

11.2　安全交换协议(SEP)

一个字节的安全交换协议参数(SEP)字段信息如下,其比特位分配见图 4。

——如果服务代码(SVC)为 00b,表示这个 PDU 是一个 SSE 交换的一部分;如果 SVC 为 01b,表示这个 PDU 是 SCH 交换的一部分。

——消息码（MSG）表示 PDU 的类型，详见表 3。

——其余的部分为预留位(RFU)。RFU 的所有比特位应设为 0。接收者应拒绝接收 RFU 比特位设置为 1 的 PDU。

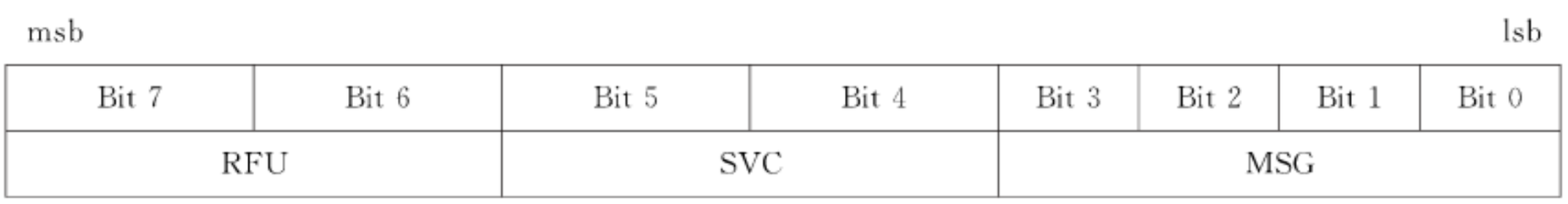

图 4　SEP 比特位分配

表 3　PDU 类型和相应的 MSG 编码

编码	名称	描述
0000	ACT_REQ	激活请求，请求新的服务
0001	ACT_RES	激活响应，接受服务的请求
0010	VFY_REQ	验证请求，提交验证值来验证发送者的共享秘密
0011	VFY_RES	验证响应，提交验证值来验证接受者的共享秘密
0100	ENC	加密数据包用于安全数据交换
0110	TMN	结束请求，结束一个服务
1111	ERROR	提示错误信息
其他		RFU

11.3　协议标识符(PID)

GB/T 33746.2—2017 定义了一个单独的 8 比特 PID，PID 只包含在 ACT_REQ 中。

11.4　NFC-SEC 有效载荷

TMN PDU 不应包含 NFC-SEC 有效载荷字段。NFC-SEC 有效载荷字段应由一个 8 位位组(字节)的整数倍组成。NFC-SEC 有效载荷字段在 ERROR PDU 中的使用可详见 11.6 错误(ERROR)的描述。NFC-SEC 有效载荷字段在其他类型 PDU 中的使用、结构以及编码可参见GB/T 33746.2—2017。

11.5　终止(TMN)

如表 2 中的描述所示，TMN PDU 只包含 SEP 字段。

11.6　错误(ERROR)

ERROR PDU 从 SEP 字段开始，如果包含有效载荷，NFC-SEC 有效载荷字段应包含一个以 0 结尾的八进制串。

12　协议规则

12.1　协议和服务错误

协议和服务错误规则包括：

——当 NFC-SEC 实体在不允许的状态下接收到一个 PDU，应发送 ERROR PDU 响应。
——当 NFC-SEC 实体接收到一个不支持的或者是在 GB/T 33746.2—2017 中定义为包含无效内容的 PDU 时，应发送 ERROR PDU 响应。
——当 NFC-SEC 实体接收或者发送 ERROR PDU 时，应把协议状态设置为空闲(Idle)。
——当 NFC-SEC 实体接收或者发送 ERROR PDU 时，应向 NFC-SEC 用户发送 ERROR SDU。
——当 NFC-SEC 实体接收到一个不支持的或者是在 GB/T 33746.2—2017 中定义为包含无效内容的 SDU 时，应发送 ERROR PDU 响应且不改变协议状态。

12.2 互通规则

互通规则包括：

——NFC-SEC 实现可设置 NFC-SEC-SDU 消息长度上限。当发送 B.2 中的请求 SDU 时，如超过消息长度上限，则此 SDU 应被拒绝。
——一个 NFC-SEC-PDU 应只包含一个 NFC-SEC-SDU。
——根据序 12.3 中的描述，NFC-SEC 实体应丢弃任何 NFC-SEC-PDU 副本。

12.3 序列完整性

GB/T 33746.2—2017 提供的序列完整性保护应遵循以下序列完整性机制：

——每一个 NFC-SEC 实体应维护其 SNV。
——SCH 建立时，接受者应初始化其 SNV，SNV 值与 GB/T 33746.2—2017 指定的发送者的 SNV 值相同。
——GB/T 33746.2—2017 规定了 SNV 值的范围。
——发送 ENC 时，NFC-SEC 实体应将 SNV 值加 1，并把它放置在 SN 字段中。
——SN 字段应受 PDU 安全机制的保护，保证任何改动都能监测到。
——接收 ENC 时，NFC-SEC 实体应解析 SN 字段并且与它的 SNV 值相比较。如果 SN 等于 SNV，则 PDU 应被丢弃而不是提交给 NFC-SEC 用户，而且状态和 SNV 应按照 B.4.4 的要求不做修改。
——NFC-SEC 实体应每次给 SNV 值增加 1。如果 SN 等于 SNV，则 B.4.4 中的“PDU 内容无效”为真；否则为假。

注：如果出现序列完整性错误，NFC-SEC 退出 SCH 并且将情况通知到对等 NFC-SEC 用户。NFC-SEC 用户可自行决定是使用新密钥重新建立 SCH 还是退出服务。

12.4 加密处理

除了 TMN 和 ERROR 情况之外，发送 PDU 之前或者接收 PDU 之后，加密处理的过程在 GB/T 33746.2—2017指定。如果接收进来的 PDU 加密处理结果为否，则附录 B 中定义的“PDU 内容有效”为假。

附 录 A
（规范性附录）
在 ISO/IEC 18092:2004（NFCIP-1）中使用 NFC-SEC 的附加要求

在 ISO/IEC 18092:2004 实现中使用本部分规定的 NFC 安全规范时，应满足以下附加要求。A.4 中说明的这些附加要求与 A.1～A.3 中的功能相关。

A.1 NFCIP-1 设备表明支持 NFC-SEC 的方法

初始方用 ATR_REQ 的 SECi 字段表明支持 NFC-SEC。
目标方用 ATR_RES 的 SECt 字段表明支持 NFC-SEC。
SECi 和 SECt 定义见 A.4。

A.2 安全 PDU 介绍

数据交换协议中增加了安全 PDU(Protected PDU)，其定义见 A.4。

A.3 安全 PDU 编号扩展规则

PDU 编号规则包括了安全 PDU ，见 A.4。

A.4 NFCIP-1 修订

以下修订应在 ISO/IEC 18092:2004 中应用：
用下面内容替换 12.5.1.1.1 中对 PPi 比特 7 的定义
“
——比特 7：SECi。如初始方支持 NFC-SEC 则设置 SECi 为 1，反之为 0。
”
用下面内容替换 12.5.1.2.1 中对 PPt 比特 7 的定义：
“
——比特 7：SECt. 如目标方支持 NFC-SEC 则设置 SECt 为 1 ，反之为 0。
”
用下面内容替换 12.6.1.1.1 中 PFB 字节 0 定义和表 24：
“
字节 0：PFB
PFB 应包含控制数据发送和错误恢复的信息位。
PFB 用于传送控制发送的信息位。
数据交换协议定义以下基本的 PDU：
——信息 PDU(Information PDU)用于传送应用层信息。
——安全 PDU(Protected PDU)用于传送加密后的信息。
——确认 PDU(Acknowledge PDU)用于传送肯定或否定的确认信息，它不包括数据域，确认信息与前一个接收的块相关。

——监控 PDU(Supervisory PDU)用于传送初始方和目标方之间的控制信息,定义了两种类型监控 PDU:

- 响应延时超长类:包含 1 个字节长度数据区域。
- 注意类:无数据区域。

PFB 编码取决于它的类型,见表 A.1。

表 A.1　PFB 比特 5 到比特 7 的编码

比特 7	比特 6	比特 5	PFB
0	0	0	信息 PDU
0	0	1	安全 PDU
0	1	0	确认 PDU
1	0	0	监控 PDU
注:其余是 RFU 定义。			

”

将安全 PDU 定义和图 A.1 添加到 12.6.1.1.1。

“

安全 PDU 定义:

RFU	RFU	ONE	MI	NAD	DID	PNI	PNI

图 A.1　安全 PDU 的编码

——比特 7 和比特 6:RFU。初始方应置为 0,目标方应忽略。

——比特 5:应置为 1。

——比特 4:置为 1,表示多信息链接(Multiple Information chaining)已激活。

——比特 3:置为 1 表示 NAD 有效。

——比特 2:置为 1 表示 DID 有效。

——比特 1 和比特 0:PNI 包编号信息。

PNI(Packet Number Information,包编号信息)是初始方和目标方之间相互发送的包数目,初值为 0,用于协议处理时的错误检测。

”

用下面内容替换 12.6.1.2 内容:

“

12.6.1.2.1　初始方规则

针对每个目标方,应将初始方的 PNI 初始化为全 0 序列。

当接收到具有相同 PNI 的 PDU 如信息 PDU、或安全 PDU 或确认 PDU 时,初始方应该在选择性地发送新帧之前,将该目标方对应的当前 PNI 值增加 1。

12.6.1.2.2　目标方规则

目标方的 PNI 应被初始化为全 0 序列。

当目标方接收到一个与当前 PNI 值相等的信息 PDU、或安全 PDU、或确认 PDU 后,则发送包含本 PNI 的响应,然后将该 PNI 值加 1。

”

用下面内容替换 12.6.1.3.1 内容：

“

12.6.1.3.1　一般规则

第一个 PDU 应由初始方发出。

当接收的 PDU 如信息 PDU 或安全 PDU 带有很多信息，则该 PDU 应由 ACK 这个确认 PDU 来确认。

监控 PDU 应成对使用，即监控请求（Supervisory Request）消息后面应有一个监控响应(Supervisory Response)消息。

”

用下面内容替换 12.6.1.3.3 内容：

“

12.6.1.3.3　目标方规则

允许目标方发送监控 PDU(RTO)而不是信息 PDU。

当接收到没有链接密钥的信息 PDU 或安全 PDU，则它们可认为是普通的信息 PDU 或安全 PDU。

当接收到 NACK 这个确认 PDU，如果其 PNI 等于先前发出的 PDU 的 PNI，先前的块应重新再发送。

当接收错误的 PDU 则目标方不应答并且状态保持不变。

当接收监控 PDU（注意类），目标方发送监控 PDU（注意类）响应。

”

附 录 B
（规范性附录）
协议机规范

本附录中的 NFC-SEC 协议机规定了建立和终止 SSE 服务以及建立、使用和终止 SCH 服务发送 PDU 的顺序。

此外，协议机还规定了在每一个状态可发送和接收的 PDU。

B.1 SDL 符号

从NFC-SEC对等实体处接收的NFC-SEC-PDU，
通过本地NFCIP-1实体来传送

发给NFC-SEC对等实体的NFC-SEC-PDU，
提交给本地NFCIP-1实体

从NFC-SEC用户处获取的NFC-SEC-SDU，
要求NFC-SEC实体执行一个操作

发给NFC-SEC用户的NFC-SEC-SDU，
作为以前请求的响应或者指明一个事件

状态。在状态中，协议机等待事件。
在构成协议错误的图表中，事件是不可预见的。

事件执行的过程中分支条件的判断。

B.2 请求 SDU

NFC-SEC 用户发送请求 SDU 来请求 NFC-SEC 业务。参数如下，其数值见 GB/T 33746.2—2017。

注：请求原语（如：呼叫方法，过程内 PDU）的具体实现方法不在本部分范围内。

服务调用(Service Invocation)	请求新业务(业务类型,PID)的标识
发送数据(Send Data)	请求要发送的数据,仅 SCH(数据)
获得数据(Retrieve Data)	请求获得接收的数据,仅 SCH
获得秘密(Retrieve Secret)	请求获得一个共享秘密连接,仅 SSE
终止(Terminate)	请求终止业务(业务类型)

B.3 确认 SDU

NFC-SEC 实体发送确认 SDU 给 NFC-SEC 用户。参数如下,其数值见 GB/T 33746.2—2017。

注:确认原语(如:呼叫方法,过程内 PDU)的具体实现方法不在本部分范围内。

建立(Established)	表示业务建立成功(业务类型)
数据发送(Data Sent)	表示发送数据请求(状态)结果。结果可能为肯定或否定,否定结果的原因可能是由于发送错误或者 NFC-SEC 实体没准备好发送
数据可用(Data Available)	表示获得数据
返回数据(Return Data)	响应获得数据请求(数据)
返回秘密(Return Secret)	响应获得秘密请求(共享秘密)
终止(Terminated)	指示用户业务(业务类型)终止
错误(Error)	表示处理请求或 PDU 过程中发生错误,参数可反映错误原因和细节(细节)

B.4 SDL 流程

B.4.1 空闲状态

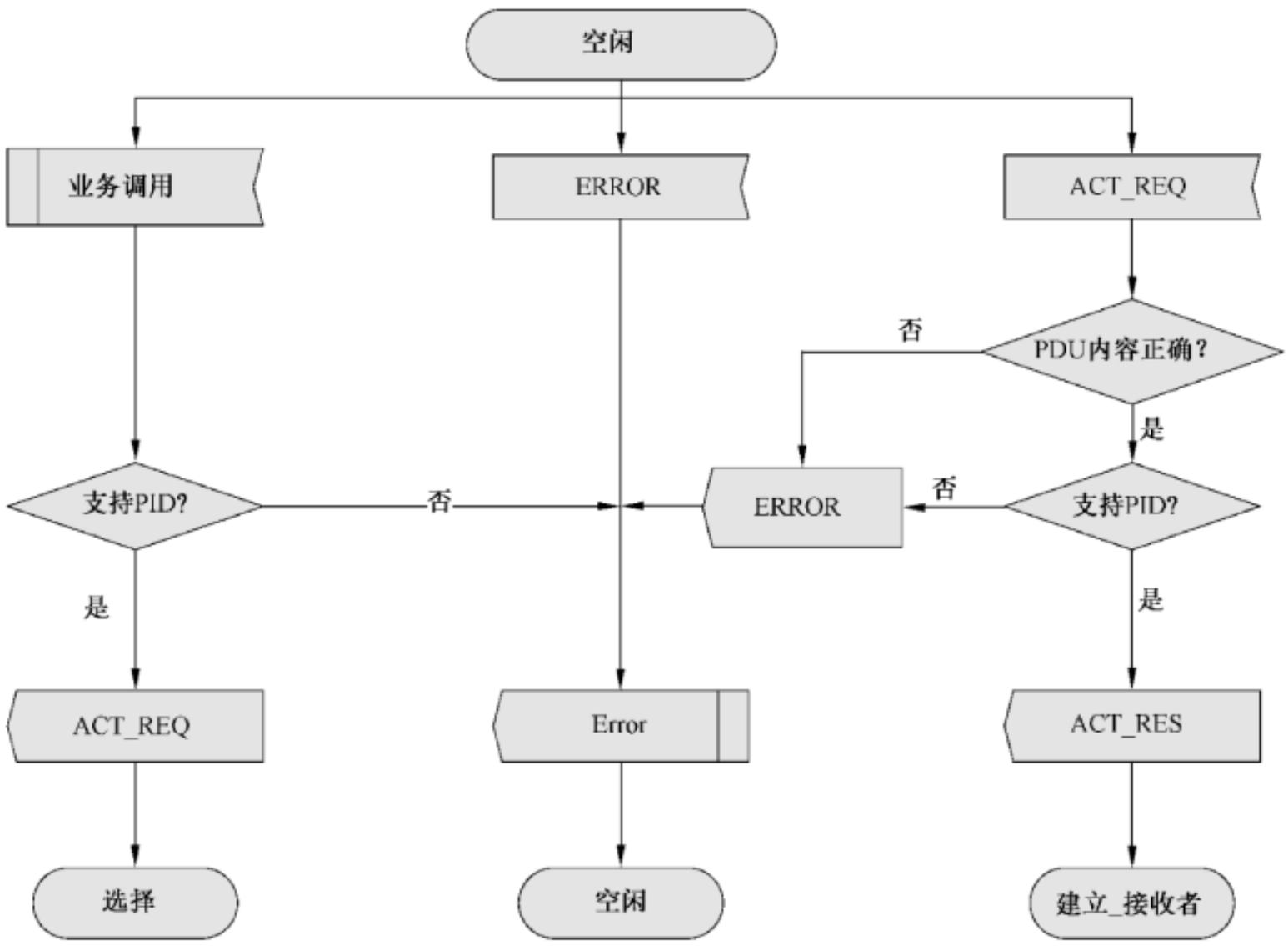

图 B.1 空闲状态的 SDL 流程

B.4.2 选择状态

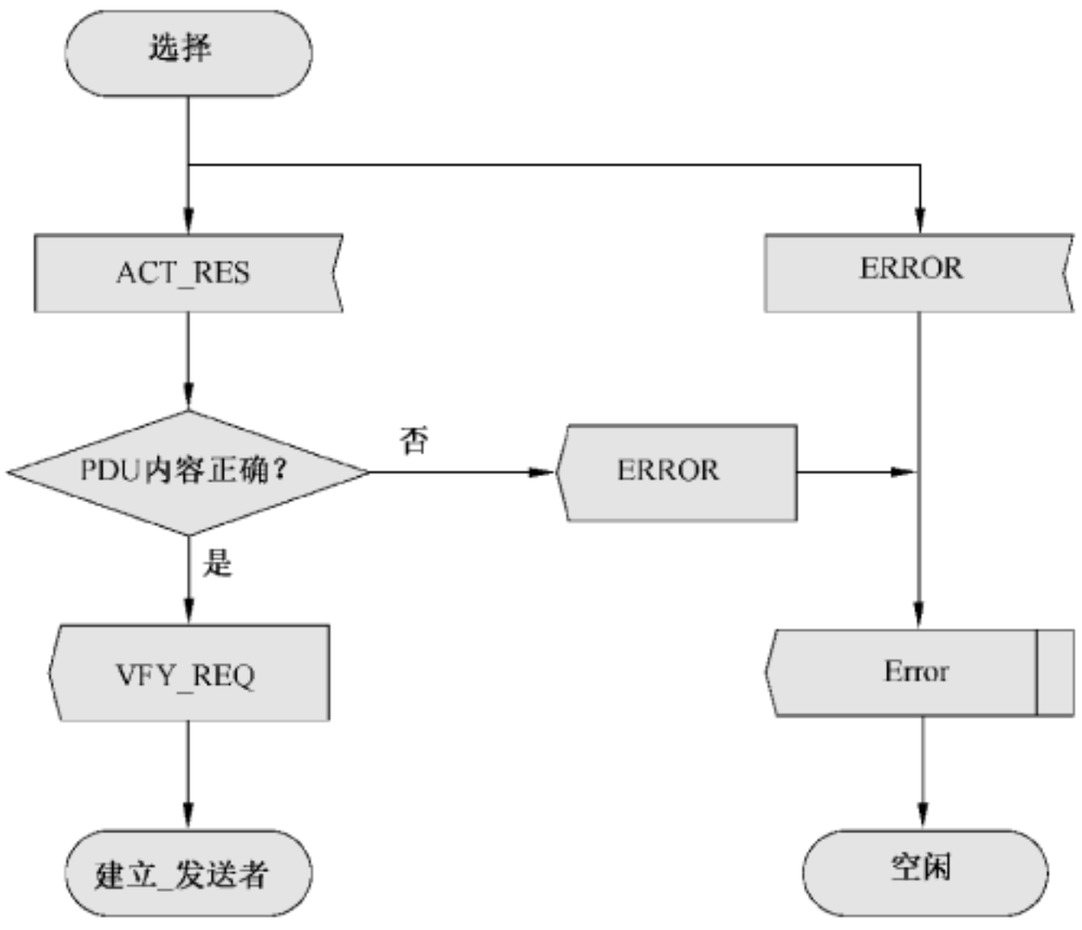

图 B.2 选择状态的 SDL 流程

B.4.3 建立状态

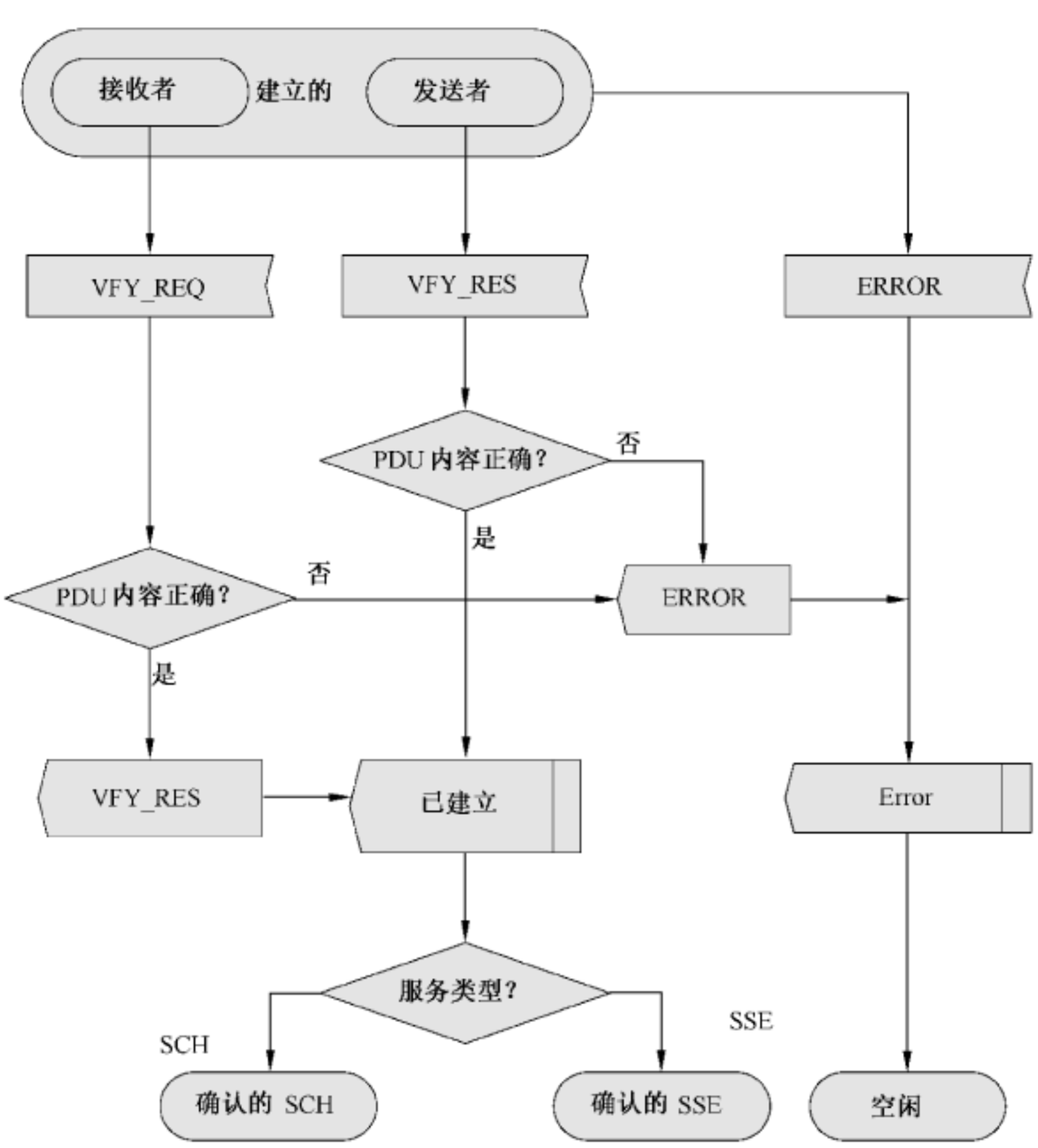

图 B.3 建立状态的 SDL 流程

B.4.4 确认状态

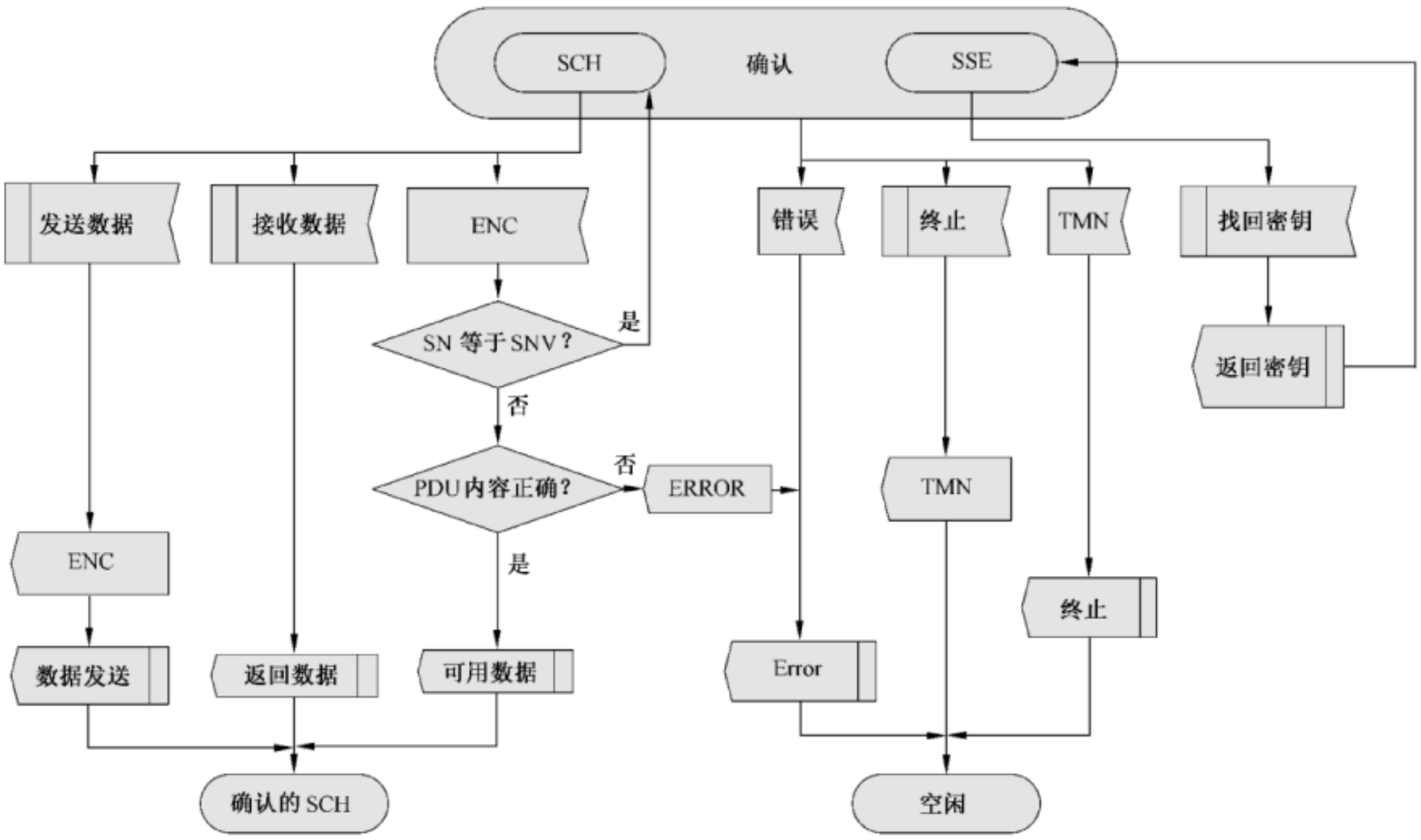

图 B.4 确认状态的 SDL 流程

中 华 人 民 共 和 国
国 家 标 准
近场通信(NFC)安全技术要求
第 1 部分:NFCIP-1 安全服务和协议
GB/T 33746.1—2017
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2017 年 9 月第一版
*
书号:155066·1-55779

GB/T 33746.1-2017