ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 18237.3—2000
idt ISO/IEC 11586-3:1996

信息技术 开放系统互连 通用高层安全 第3部分:安全交换服务元素(SESE)协议规范

Information technology—Open Systems Interconnection—Generic upper layers security—Part 3:Security Exchange Service Element (SESE) protocol specification

2000-10-17 发布　　2001-08-01 实施

国家质量技术监督局 发布

目　　次

前　言

本标准等同采用国际标准 ISO/IEC 11586-3:1996《信息技术　开放系统互连　通用高层安全:安全交换服务元素(SESE)协议规范》。

GB/T 18237 在《信息技术　开放系统互连　通用高层安全》的总标题下,目前包括以下几个部分:

第 1 部分(即 GB/T 18237.1):概述、模型和记法

第 2 部分(即 GB/T 18237.2):安全交换服务元素(SESE)服务定义

第 3 部分(即 GB/T 18237.3):安全交换服务元素(SESE)协议规范

第 4 部分(即 GB/T 18237.4):保护传送语法规范

附录 A 和附录 B 是标准的附录。

本标准由中华人民共和国信息产业部提出。

本标准由中国电子技术标准化研究所归口。

本标准起草单位:中国电子技术标准化研究所。

本标准主要起草人:郑洪仁、张　莺。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(他们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术范围的国际标准。ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系的其他官方和非官方国际组织也可参与国际标准的制定工作。

对于信息技术,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC 1。由联合技术委员会提出的国际标准草案需分发给国家成员体进行表决。发布一项国际标准,至少需要 75%的参与表决的国家成员体投票赞成。

国际标准 ISO/IEC 11586-3 是由 ISO/IEC JTC 1"信息技术"联合技术委员会的 SC 21"开放系统互连、数据管理和开放分布式处理"分技术委员会与 ITU-T 共同制定的。等同文本为 ITU-T 建议 X.832。

ISO/IEC 11586 在《信息技术　开放系统互连　通用高层安全》总标题下,目前包括以下 6 个部分:

——第 1 部分:概述、模型和记法

——第 2 部分:安全交换服务元素(SESE)服务定义

——第 3 部分:安全交换服务元素(SESE)协议规范

——第 4 部分:保护传送语法规范

——第 5 部分:安全交换服务元素协议实现一致性声明(PICS)形式表

——第 6 部分:保护传送语法协议实现一致性声明(PICS)形式表

附录 A 和附录 B 构成为本标准的一部分。

引　　言

本标准是系列标准的一个部分，这个系列标准给出了一组设施，以帮助构造支持提供安全服务的高层协议。本系列标准的各部分如下：

——第 1 部分：概述、模型和记法；

——第 2 部分：安全交换服务元素服务定义；

——第 3 部分：安全交换服务元素协议规范；

——第 4 部分：保护传送语法规范；

——第 5 部分：安全交换服务元素 PICS 形式表；

——第 6 部分：保护传送语法 PICS 形式表。

本标准为该系列标准的第 3 部分。

中华人民共和国国家标准

信息技术　开放系统互连　通用高层安全 第3部分：安全交换服务元素（SESE）协议规范

GB/T 18237.3—2000
idt ISO/IEC 11586-3:1996

Information technology—Open Systems Interconnection—Generic upper layers security—Part 3:Security Exchange Service Element (SESE) protocol specification

1 范围

1.1 本系列标准定义了一组用于辅助在应用层协议中提供安全服务的通用设施。它们包括：

a）一组记法工具，这组工具用来支持抽象语法规范中的选择字段保护需求的规范，以及支持安全交换和安全变换规范；

b）应用服务元素（ASE）的服务定义、协议规范和 PICS 形式表，它们支持在 OSI 的应用层内提供的安全服务；

c）安全传送语法的规范和 PICS 形式表，这些语法与支持应用层中的安全服务的表示层相关。

1.2 本标准定义了由安全交换服务元素（SESE）提供的协议。该 SESE 是一个允许安全信息通信以支持在应用层内提供安全服务的 ASE。

2 引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 17965—2000　信息技术　开放系统互连　高层安全模型（idt ISO/IEC 10745:1995）

GB/T 18237.2—2000　信息技术　开放系统互连　通用高层安全　第2部分：安全交换服务元素（SESE）服务定义（idt ISO/IEC 11586-2:1996）

ISO/IEC 8824-2:1995　信息技术　抽象语法记法1（ASN.1）：信息客体规范

ISO/IEC 8824-4:1995　信息技术　抽象语法记法1（ASN.1）：ASN.1规范的参数化

3 定义

本标准采用 GB/T 17965 中定义的下列术语：

——安全交换　security exchange

——安全交换项　security exchange item

4 缩略语

ACSE　联系控制服务元素

APDU　应用协议数据单元

ASE　应用服务元素

国家质量技术监督局 2000-10-17 批准　　2001-08-01 实施

ASO 应用服务客体
OSI 开放系统互连
PICS 协议实现一致性声明
SEI 安全交换项
SEPM 安全交换协议机
SESE 安全交换服务元素

5 协议概述

5.1 服务措施

本规范中定义的协议提供了 GB/T 18237.2 中定义的服务。这些服务如下：

SE-TRANSFER 非证实型
SE-U-ABORT 非证实型
SE-P-ABORT 提供者发起型

5.2 下层服务的用法

这种 SESE 协议定义了一组 APDU，根据有效的 ASO 上下文或应用上下文规则，其中每一个 APDU 可能映射到运送用户数据的任何表示层服务，或者其可以被嵌入进或拼接到其他任何应用 PDU。

第 8 章定义了一些到表示服务和 ACSE 的有用映射。

6 规程的元素

6.1 使用的 APDU

SESE 协议规定了下列 APDU：

SE-TRANSFER APDU(SETR)
SE-U-ABORT APDU(SEAB)
SE-P-ABORT APDU(SEPA)

6.2 传送规程

这种规程由请求者 SEPM 用来发起要求传送一个或多个安全交换项的安全交换。这种规程也可以由请求者 SEPM 或响应者 SEPM 用来传送由请求者启动的另外的安全交换项。

一旦收到 SE-TRANSFER request 原语，SEPM 就保留安全交换标识符，并生成一个 SE-TRANSFER APDU (SETR)。

一旦收到 SE-TRANSFER APDU (SETR)，SEPM 就保留安全交换标识符，并发出 SE-TRANSFER indication 原语。

如果安全交换属于“交替”类，并且该交替不遵循预期的顺序，则 SEPM 生成 SE-P-ABORT APDU (SEPA)，并发出 SE-P-ABORT indication 原语。

6.3 用户发起型夭折规程

这种规程由一个 SESE 用户使用以向对等的 SESE 用户和 SEPM 指出差错已出现，并且在进程中的任何安全交换都被非正常终止。此外，它可能会导致具有传送中信息丢失的 ASO 联系的非正常释放。它是由 SE-U-ABORT request 原语发起的。

一旦收到 SE-U-ABORT request 原语，SEPM 就生成 SE-ABORT APDU(SEAB)。

一旦收到 SE-ABORT APDU (SEAB)，SEPM 就发出 SE-U-ABORT indication 原语。

6.4 提供者发起型夭折规程

这种规程由 SEPM 使用以向 SESE 用户指出差错已出现，并且在进程中的任何安全交换都被非正常终止。此外，它可能导致在传送中出现信息丢失的 ASO 联系的非正常释放。

一旦检测到差错，SEPM 就发出 SE-P-ABORT indication 原语，并生成 SE-P-ABORTAPDU

(SEPA)。如果差错严重到要求终止 ASO 联系,则 SEPA APDU 被映射到 ASO 联系夭折服务。在收到具有 SEPA APDU 的 ASO 联系夭折指示时,SEPM 便发出具有严重性指示符置位的 SE-P-ABORT indication。

引起 SE-P-ABORT 生成的差错条件具有相关的问题代码,它可以向两端指示。指示的问题分为如下几类:

a) 一般问题——不限于任一特定的 APDU 类型;

b) 传送问题——由收到 SE-TRANSFER APDU 引起的问题;

c) 夭折问题——由收到 SE-ABORT APDU 引起的问题。

特定的差错条件,以及联系的问题代码叙述如下:

6.4.1 一般问题

无效 APDU——APDU 的结构和/或编码与 SETR、SEAB 或 SEPA APDU 都不符。

6.4.2 传送问题

a) 重复的调用标识符——与另一个活跃的安全交换调用正在使用的标识符相同的调用标识符;

b) 不可识别的安全交换——所标识的安全交换对这个 ASO 上下文无效;

c) 错误类型的项——SEI 的类型与客体类定义中的类型不符;

d) 不适当的调用标识符——该调用标识符不属于为这个 ASO 上下文规定的标识符;

e) 交替顺序错——所收到的 SETR 没有遵循安全交换"交替"类的顺序。

6.4.3 夭折问题

a) 不可识别的调用标识符——调用标识符未标识出活跃的或刚刚完成的安全交换传送;

b) 非预期夭折——所标识的安全交换未生成这个安全交换项的夭折;

c) 不可识别的差错——所标识的安全交换未生成这种差错;

d) 非预期的差错——所标识的安全交换未生成这个安全交换项的差错;

e) 错误类型的差错参数——差错参数的类型与该差错定义的类型不符。

7 SESE APDU 的结构和编码

通用 SESE APDU 的参数化数据类型是使用 ASN.1(见 ISO/IEC 8824-4)在 7.1 中规定的。支持特定安全交换集构造 SESE 抽象语法的方法在 7.2 中描述。

7.1 通用 APDU 规范

下面的参数化 APDU 规范支持用于特定的 SESE 的抽象语法定义,且该 SESE 支持使用本系列标准第 1 部分中的规范框架定义的任一组安全交换。在下面,参数 ValidSEs 标识了被支持的一组安全交换。参数 InvocationIdSet 定义了一些可用值,这些值用来标识可以同时活跃的不同安全交换调用,并且用来使随后的响应和差错指示与现行安全交换调用相关。如果这种相关在某些实现中是不需要的(例如,不同的安全交换调用不会重叠),则 InvocationIdset 应被置成设定的值 NoInvocationId。

```
SeseAPDUs{joint-iso-ccitt genericULS(20)modules(1)seseAPDUs(6)}
DEFINITIONS AUTOMATIC TAGS::=
BEGIN
--全部 EXPORTS--
IMPORTS
        Notation
          FROM ObjectIdentifiers {joint-iso-ccitt genericULS(20)
            modules(1)objectIdentifiers(0)}
        dirAuthenticationTwoWay
```

```
    FROM GulsSecurity Exchanges{joint-iso-ccitt genericULS(20)
      modules(1)gulsSecurityExchanges(2)}
  SECURITY-EXCHANGE{},SE-ERROR{}
    FROM NOTATION notation;
SESEapdus{SECURITY-EXCHANGE:ValidSEs,InvocationId:InvocationIdSet}::=
  CHOICE{
    se-transfer          SETransfer{{ValidSEs},{InvocationIdSet}},
    se-u-abort           SEUAbort{{ValidSEs},{InvocationIdSet}},
    se-p-abort           SEPAbort{{ValidSEs},{InvocationIdSet}}
    }
SETransfer{SECURITY-EXCHANGE:ValidSEs,InvocationId:InvocationIdSet}::=
SEQUENCE{
    seIdentifier     SECURITY-EXCHANGE.&SE-Identifier{ValidSEs}),
                     ——它标识出由特定 SESE 抽象语法
                     ——所支持的安全交换之一
    itemIdentifier   SECURITY-EXCHANGE.&SE-Items.&itemId
                     ({ValidSEs}{@seIdentifier}),
                     ——它标识出由“seIdentifier”指出的
                     ——安全交换的安全交换项之一
    seItem           SECURITY-EXCHANGE.&SE-Items.&ItemType
                     ({ValidSEs}{@seIdentifier,@itemIdentifier}),
    invocationId     InvocationId(InvocationIdSet)
                     (CONSTRAINED BY{——如果起始标志不为真,则它必须与活跃安
                     全交换的 invocationId 相同})
                     DEFAULT noInvocationId,
    startFlag        BOOLEAN DEFAULT FALSE,
                     ——仅当作为传送安全交换的第一个安全交换项时
                     ——才设置此字段。
    endFlag          BOOLEAN DEFAULT FALSE
                     ——当作为传送安全交换的最后一个安全交换项时
                     ——设置此字段。需要提供需求 n 次交换的这些机制,
                     ——其中 n 是事先未知的——}
SEUAbort{SECURITY-EXCHANGE:ValidSEs,InvocationId:InvocationIdSet}::=
SEQUENCE{
    InvocationId     InvocationId{InvocationIdSet}
                     (CONSTRAINED BY{——它必须与活跃或刚完成的
                     ——安全交换的 invocationId 相同——})
                     DEFAULT noInvocationId,
    ItemIdentifier   SECURITY-EXCHANGE.&SE-Items.&itemId
                     ({ValidSEs.&SE-Items})OPTIONAL,
                     ——这个成份仅当在收到 SETransferAPDU 之后
                     ——生成夭折时才出现,
```

```
        errors          SEQUENCE OF SEerror{{ValidSEs}} OPTIONAL
                        ——需要处理多个差错代码——}
    SEPAbort {SECURITY-EXCHANG:ValidSEs,InvocationId:InvocationIdSet}::=
    SEQUENCE{
        invocationId    InvocationId(InvocationIdSet)OPTIONAL,
        itemIdentifier  SECURITY-EXCHANGE.&SE-Items.&itemId
                        ({ValidSEs,&SE-Items})OPTIONAL,
                            ——这个成份仅当在收到 SETransferAPDU 之后
                            ——生成夭折时才出现,
        problemCode     ProblemCode}
    INVOCATIONId::=CHOICE{
        present           INTEGER,
        absent          NULL}
    noInvocationId InvocationId::=absent:NULL
    NoInvocationId InvocationId::={noInvocationId}
    SEerror{SECURITY-EXCHANGE:ValidSEs}::=SEQUENCE{
        errorCode       SE-ERROR.&errorCode
                        ({Errors{{ValidSEs}}})OPTIONAL,
        errorParam-     SE-ERROR.&ParameterType
        eter            ({Errors{{ValidSEs}}}{@errorCode})OPTIONAL}
      Errors {SECURITY-EXCHANGE: ValidSEs } SE-ERROR:: = { ValidSEs. &SE-Items.
&Errors}
    ProblemCode::=CHOICE{
        general         GeneralProblem,
        transfer        TransferProblem,
        abort           AbortProblem}
    GeneralProblem::=ENUMERATED{
        invalidAPDU(0)}
    TransferProblem::=ENUMERATED{
        duplicateInvocationId(0),
        unrecognizedSecurityExchange(1),
        mistypedItem(2),
        inappropriateInvocationId(3),
        alternatingSequenceError(4)}
    AbortProblem::=ENUMERATED{
        unrecognizedInvocationId(0),
        abortUnexpected(1),
        unrecognizedError(2),
        unexpectedError(3),
        mistypedErrorParameter(4)}
    END
```

7.2 抽象语法的构造

用于支持给定安全交换集的 SESE 的抽象语法可使用 ISO/IEC 8824-2 附录 B 中定义的 AB-

STRACT-SYNTAX 信息客体类来规定。

例如，为了规定支持本系列标准第 1 部分的附录 D 和附录 I 中定义的其中两种安全交换的 SESE 抽象语法，对于不要求调用标识符的实现，应使用下列记法：

```
AccCtl-Authentication-Abstract-Syntax
ABSTRACT-SYNTAX::=
  {SESEapdus{
    {boundAccessControlCert|dirAuthenticationTwoWay},
    NoInvocationId}
  IDENTIFIED BY{…Abstract Syntax ObjectIdentifier…}
```

8 到下层服务的映射

8.1 概述

SESE 协议定义了一组 APDU，根据有效的 ASO 上下文或应用上下文的规则，其中每一个 APDU 可能映射到运送用户数据的任何表示层服务，或者其可以嵌入进或拼接到其他任何 APDU。

除非在 ASO 上下文(或应用上下文)定义中另有规定，当 SETR 映射到 P-DATA 服务时，则具有严重性指示符置位的 SEAB 或具有严重到要求非正常终止联系的差错的 SEPA 被映射到 A-ABORT 服务。

如果应用上下文规范中业已包括 SESE，则在这个应用上下文中既不要求，也不阻止包括 ACSE 鉴别功能单元。

SESE 不能直接使用其他 ASE，但只能借助于控制功能间接使用其他 ASE(像在应用层结构中指出的那样)。已规定的一些有用的映射例子如下。

8.2 到 ACSE 服务的映射

8.2.1 SE-TRANSFER 到 A-ASSOCIATE 的映射

当最前面一个或两个安全交换传送与联系建立一同出现时，则 SE-TRANSFER APDU 可被映射到 A-ASSOCIATErequest/indication 的鉴别值字段或用户信息字段。

当 SE-TRANSFER APDU 是应答 A-ASSOCIATE request/indication 运送的 SE-TRANSFER APDU 时，则前面的 SE-TRANSFER APDU 可被映射到 A-ASSOCIATEresponse/confirm 的鉴别值字段或用户信息字段。

当 SE-TRANSFER APDU 被映射到 A-ASSOCIATE 的鉴别值字段时，则应使用 EXTERNAL 选项，且不应使用鉴别机制名字段。

8.2.2 附加 SE-TRANSFER 的映射

当与联系建立一同出现的安全交换要求传送两个以上的安全交换项时，则第三个和第三个以上的传送(SE-TRANSFER)可被映射到 P-DATA。在这种情况下，该应用上下文可能具有这样一个规则，那就是，即使这一联系在前两个传送之后被成功地建立起来，但直到成功地完成安全交换时才可由其他 ASE 使用。

9 一致性

声称实现本标准中规定的规程的系统应符合 9.1 到 9.3 中的各项要求。

9.1 声明要求

实现者应声明如下内容：

a) 所提供的一组安全交换；

b) 对于所提供的每一个安全交换，该系统是否能发起该安全交换和/或响应由另一端发起的安全交换；

c) 能同时生成/活跃的调用标识符的范围；

d) 该系统是否能支持安全交换的“交替”和/或“任意”类。

9.2 静态要求

该系统应：

a) 对一个或多个安全交换起发起者和/或响应者的作用；

b) (至少)要支持通过把基本 ASN.1 编码规则施用于第 7 章中规定的 ASN.1 而进行的编码，以达到交换 SESE APDU 的目的。

9.3 动态要求

该系统应遵守第 6 章中规定的全部规程。

附 录 A
（标准的附录）
SEPM 状态表

A1 概述

本附录以状态表形式定义了定全交换协议机(SEPM)。这种状态表示出了 SEPM 状态、协议中的入事件、采取的动作，以及与 SEPM 结果状态之间的相互关系。

该 SEPM 状态表没有建立 SEPM 的形式定义。它包含比第 6 章中规定的规程元素更明确的规范。这个附录与第 6 章同等重要。该规范中的任何一个冲突都应作为一个差错来对待。

本附录包括下列几种表：

a) 表1 规定了每个入事件的缩写名、源和名称。这些源是：

1) SEPM 服务用户(SE 用户)；

2) 对等 SEPM(SE 对等)。

b) 表2 规定了每个出事件的缩写名、目标和名称。这些目标是：

1) SEPM 服务用户(SE 用户)；

2) 对等 SEPM(SE 对等)。

c) 表 3 规定了所使用的谓词。

d) 表 4 规定了每个状态的缩写名和说明。

e) 表 5 规定了使用上述各表缩编而成的 SEPM 状态表。

A2 约定

入事件(状态表中的行)和状态(状态表中的列)的交叉处形成一个单元。

在状态表中，空白单元表示入事件与状态的组合没有对 SEPM 进行定义。

非空白单元表示入事件和状态已对 SEPM 进行了定义。这种单元应包含一个动作列表(必备的和/或有条件的)。

A3 表

表 A1 入事件列表

缩 写 名	源	名
SE-TRANSFERreq	SE 用户	SE-TRANSFERreq 原语
SETR	SE 对等	SE-TRANSFER APDU
SE-U-ABORTreq	SE 用户	SE-U-ABORTreq 原语
SEAB	SE 对等	SE-U-ABORT APDU
SEPA	SE 对等	SE-P-ABORT APDU
无效 APDU	SE 对等	无效 APDU

表 A2 出事件列表

缩 写 名	目标	名
SE-TRANSFERind	SE 用户	SE-TRANSFERind 原语
SETR	SE 对等	SE-TRANSFER APDU
SE-U-ABORTind	SE 用户	SE-U-ABORTind 原语
SEAB	SE 对等	SE-U-ABORT APDU
SEPA	SE 对等	SE-P-ABORT APDU
SE-P-ABORTind	SE 用户	SE-P-ABORTind 原语

表 A3 谓词

代 码	含 意
p1	EndFlag＝真
p2	检测到的传送问题
p3	检测到的夭折问题

表 A4 SEPM 状态

缩写名	说 明
STA 0	空闲状态
STA 1	交换状态

表 A5 SEPM 状态表

	STA 0 空闲状态	STA 1 交换状态
SE-TRANSFERreq	p1 SETR STA0 ^ p1 SETR STA1	p1 SETR STA0 ^ p1 SETR STA1
SETR	p2 SE-P-ABORTind SEPA STA0 ^ p2&.p1 SE-TRANSFERind STA0 ^ p2&.^ p1 SE-TRANSFERind STA1	p2 SE-P-ABORTind SEPA STA0 ^ p2&.p1 SE-TRANSFERind STA0 ^ p2&.^ p1 SE-TRANSFERind STA1

表 A5(完)

	STA 0 空闲状态	STA 1 交换状态
SE-U-ABORTreq		SEAB STA0
SEAB		p3 SE-P-ABORTind SEPA STA0 ^ p3 SE-U-ABORTind STA0
SEPA	SE-P-ABORTind STA0	SE-P-ABORTind STA0
无效 APDU	SE-P-ABORTind SEPA STA0	SE-P-ABORTind SEPA STA0
注：未在表 5 中反映出的其他所有情况均作为对 SEPM 的本地情况来处理。		

附 录 B
(标准的附录)
基本 SESE 应用上下文定义

本附录定义了仅包含 ACSE 和 SESE 的应用上下文。这种应用上下文在开发安全服务器应用时是有用的。

B1 应用上下文名

{joint-iso-itu-t genericULS(20)application-contexts(7)basic(1)}

B2 应用服务元素

ACSE 和 SESE。

B3 SESE APDU 映射

a) SE-U-ABORT 和 SE-P-ABORT APDU 总会引起下层应用联系的非正常终止，并且总是映射到 A-ABORT 服务原语的用户信息参数；

b) 对于一次安全交换，发起者应将 SE-TRANSFER APDU 映射到 A-ASSOCIATErequest 服务原语的用户信息参数。响应者应按下列之一处理：

——发送具有“拒绝(瞬时)”结果的 A-ASSOCIATEresponseAPDU，指示在没有建立联系的情况下就成功地完成了交换；

——在差错时，夭折与上述(在 a)中)SE-U-ABORT 或 SE-P-ABORT APDU 的联系；注意，A-ABORT 服务规程碰撞是不可能的，因为发起者在这种情形下不会发出 A-ABORT。

c) 对于所有其他情况，发起者应将 SE-TRANSFER APDU 映射到 A-ASSOCIATErequest 服务原语的用户信息参数。响应者应按下列之一处理：

——发送具有空(如果发起者是发送下一个 SEI)或(更通常)包含 SE-TRANSFER APDU 的用户信息字段,以及"接受"结果的 A-ASSOCIATE response APDU。

——在差错时,规程同上述 b)的第二段。

其余 SE-TRANSFER APDU 被映射到 P-DATA;注意,SESE 是 P-DATA 服务的唯一用户。

使用上述 a)的 SE-U-ABORT 和 SE-P-ABORT 指出各种差错。注意,某些安全交换可以允许异步发送 SEI(即不执行严格的乒乓式排序)。在这种情况下,能够发生 A-ABORT 服务规程碰撞,而在这种情况下,SE-U-ABORT 或 SE-P-ABORT APDU 不应被交付给对等实体。但是,要使两个实体都意识到,该联系已被释放。

B4 PDV 拼接限制

不适用;SESE 是 P-DATA 服务的唯一用户。

B5 PDV 嵌入限制

因为 SESE 是 P-DATA 服务的唯一用户,所以只有在 SESE APDU 中嵌入的 PDV 是因使用 PROTECTED 参数化类型引起的。

B6 规程限制

除了对 ACSE 规程有限制外,没有其他限制。

B7 表示上下文限制

没有。

注:对 SESE APDU 的上下文局限于 BER 是合理的,以便简化软件开发者的任务。当然,在由 PROTECTED 类型产生的 EMBEDDED PDU 内,任何上下文都能使用。

中 华 人 民 共 和 国
国 家 标 准
信息技术 开放系统互连 通用高层安全
第3部分:安全交换服务元素(SESE)
协 议 规 范
GB/T 18237.3—2000
*
中国标准出版社出版
北京复兴门外三里河北街16号
邮政编码:100045
电 话:68522112
中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行 各地新华书店经售

*
开本 880×1230 1/16 印张 1¼ 字数 26 千字
2001年3月第一版 2001年3月第一次印刷
印数 1—1 500
*
书号:155066·1-17437 定价 13.00 元
*
科 目 562—539

GB/T 18237.3-2000