ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 18237.2—2000
idt ISO/IEC 11586-2:1996

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

Information technology—Open Systems Interconnection—Generic upper layers security—Part 2:Security Exchange Service Element (SESE) service definition

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 11586-2:1996《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)服务定义》。

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

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 11586-2 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.831。

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

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 2 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2部分:安全交换服务元素(SESE)服务定义

GB/T 18237.2—2000
idt ISO/IEC 11586-2:1996

Information technology—Open Systems Interconnection—Generic upper layers security—Part 2:Security Exchange Service Element (SESE) service definition

1 范围

1.1 这个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,这些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)提供的服务。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 18237.1—2000 信息技术　开放系统互连　通用高层安全　第1部分:概述、模型和记法(idt ISO/IEC 11586-1:1996)

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

本标准使用下列缩略语:

ASE　应用服务元素

OSI　开放系统互连

PICS　协议实现一致性声明

SEI　安全交换项

国家质量技术监督局2000-10-17批准　　2001-08-01实施

SESE 安全交换服务元素

5 约定

第 7 章使用表格形式来表示 SESE 服务原语参数。每个参数使用下列符号表示：

M 参数的出现是必备的

O 参数的出现是 SESE 协议机选项

U 参数的出现是 SESE 服务用户选项

C 参数的出现是有条件的

(=) 这个参数的值与前面 SESE 服务原语的相应参数的值等同

6 服务概述

安全交换服务元素保证与任何安全交换(已在第 1 部分中描述)有关的信息通信。这种服务一般用于鉴别、访问控制、抗抵赖或安全管理信息的传送。

6.1 特定的服务设施

定义了下列服务设施：

a) SE-TRANSFER；

b) SE-U-ABORT；

c) SE-P-ABORT。

SE-TRANSFER 服务设施被用于发起特定类型的安全交换，传送第一个安全交换项(SEI)，以及传送安全交换的其他 SEI。它是完成安全交换所要求的唯一安全设施。

SE-U-ABORT 服务设施由 SESE 服务用户使用以指出差错已出现。这种服务被用于非正常地终止进程中的安全交换。这种服务也可以有选择地非正常终止 ASO 联系。

SE-P-ABORT 服务设施由 SESE 服务提供者使用以指出差错已出现。这种服务被用于非正常地终止进程中的安全交换。这种服务也可以有选择地非正常终止 ASO 联系。

6.2 SE-TRANSFER 服务设施的规程模型

本系列标准的第 1 部分定义了下列安全交换的规程模型：

初始安全交换项(SEI)从 A 传送到 B。根据 SE-TRANSFER 中标识的具体安全交换，可选择后随一个还是多个 A 与 B 间的 SEI 传送。当收到由服务用户或服务提供者任一方生成的差错指示时，序列可在收到任何 SEI 时终止。

下面时序图举例说明了 n 次安全交换在交替方向上 SEI 传送序列的特例。(这是在 GB/T 18237.1 的 6.1 中定义的“交替的”交换类例子)。

SE-TRANSFER request

.....

SE-TRANSFER indication

SE-TRANSFER request

.....

SE-TRANSFER indication

.

.

.

SE-TRANSFER request

.....

SE-TRANSFER indication

7 服务定义

SESE 服务原语具有下列类型：

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

7.1 服务原语的参数

下面描述了服务原语参数。

7.1.1 安全交换标识符

这个参数标识出正被发起的特定安全交换类型。该标识符是使用第 1 部分中定义的 SECURITY-EXCHANGE 信息客体类在定义安全交换时确定的。

7.1.2 调用标识符

这个参数标识出特定的安全交换调用。它被用于在 SE-TRANSFER、SE-U-ABORT，或 SE-P-ABORT 原语中进行后续相关调用的查询。

调用标识符在处理上下文内的多重安全交换调用(例如应用联系)时特别有用。

调用标识符是由发起安全交换的服务用户提供的，并且确保这些标识符在所有活跃安全交换调用范围内的无二义性是这些用户的职责。

7.1.3 安全交换项

由安全交换标识符隐含的待运送项。

7.1.4 项标识符

在 SE-TRANSFER 原语中，这个参数指出这个原语正在运送哪个安全交换项。在 SE-U-ABORT 或 SE-P-ABORT 原语中，这个参数指出已检测到差错条件的安全交换项。

安全交换规范可以对“项标识符”的使用给出具体限制。确保这些限制得到满足是 SESE 用户的职责。

7.1.5 起始标志

在 SE-TRANSFER 原语中，这个参数用来指出安全交换的第一个安全交换项的传送。

7.1.6 结束标志

在 SE-TRANSFER 原语中，这个参数用来指出这个安全交换对应于满足该安全机制所要求的最后一个安全交换。需要提供要求 n 次交换的那些机制，其中 n 是预先不知道的。

7.1.7 差错表

这个参数是一个或多个差错代码(具有可选差错参数)的列表。该差错代码指出 SE-U-ABORT 生成的原因。当定义安全交换时，使用第 1 部分中定义的 SE-ERROR 信息客体类来建立差错代码。可选差错参数提供了描述夭折原因的附加信息。

7.1.8 问题代码

这个参数指出 SE-P-ABORT 生成的原因。在第 3 部分的第 6 章中规定了一组可能的值。

7.1.9 严重性指示符

在 SE-U-ABORT request 原语中，这个参数用来向 SESE 服务提供者指示是否必须终止 ASO 联系(例如应用联系)。

在 SE-U-ABORT indication 和 SE-P-ABORT indication 原语中，这个参数用来向 SESE 服务用户指示是否必须终止 ASO 联系(例如应用联系)。

7.2 服务原语

所提供的 SESE 服务原语参数如下(对 SESE 服务的定义参见 6.1，对专门参数的描述参见 7.1)。

7.2.1 SE-TRANSFER 服务

SE-TRANSFER 服务的参数如下：

参 数 名	Req	Ind
安全交换标识符	M	M(=)
调用标识符	U	C(=)
安全交换项	M	M(=)
项标识符	U	C(=)
起始标志	U	C(=)
结束标志	U	C(=)

7.2.2 SE-U-ABORT 服务

SE-U-ABORT 服务的参数如下：

参 数 名	Req	Ind
调用标识符	U	C(=)
项标识符	U	C(=)
差错表	U	C(=)
严重性指示符	U	C(=)

7.2.3 SE-P-ABORT 服务

SE-P-ABORT 服务的参数如下：

参 数 名	Ind
调用标识符	O
项标识符	O
问题代码	M
严重性指示符	O

8 排序信息

在本服务定义中规定的唯一排序限制是，具有相同调用标识符的 SE-TRANSFER 原语调用必须与 7.1.2 一致。

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2部分:安全交换服务元素(SESE)
服 务 定 义
GB/T 18237.2—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 3/4 字数 12 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:155066·1-17434 定价 10.00 元
*
科 目 562—538

GB/T 18237.2-2000