

ICS 35.100.01
L 79



中华人民共和国国家标准

GB/T 18237.4—2003/ISO/IEC 11586-4:1996

GB/T 18237.4—2003/ISO/IEC 11586-4:1996

信息技术 开放系统互连 通用高层安全 第4部分:保护传送语法规范

Information technology—Open systems interconnection—
Generic upper layers security—
Part 4:Protecting transfer syntax specification

(ISO/IEC 11586-4:1996, IDT)

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4部分:保护传送语法规范
GB/T 18237.4—2003/ISO/IEC 11586-4:1996

*
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:68523946 68517548

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 1 字数 17 千字
2003年10月第一版 2003年10月第一次印刷
印数 1—2 000

*
书号:155066·1-19934 定价 12.00 元
网址 www.bzcbbs.com

版权专有 侵权必究
举报电话:(010)68533533



GB/T 18237.4-2003

2003-07-02 发布

2003-10-01 实施

中华人民共和国
国家质量监督检验检疫总局 发布

果发生这种情况,则要对发送实体再同步,以便使动态参数重新建立起正确的值。

9 客体标识符分配

给本部分中定义的保护传送语法分配如下客体标识符:

{joint-iso-itu-t genericULS(20)generalTranferSyntax(2)}

这种客体标识符的用法没有要求一组特定编码规则用来对 SyntaxStructure ASN.1 值进行编码,但 ASN.1 基本编码规则应按缺省使用。

当一组特定编码规则必须用来对 SyntaxStructure ASN.1 值进行编码时,为了使用,则要给本部分中定义的保护传送语法分配附加客体标识符。可以约定标准 ASN.1 编码规则规范(例如在 ISO/IEC 8825-1:1995 中定义的那些规范)中的任一个。应使用下列约定。该客体标识符用下列前缀开始:

{joint-iso-itu-t genericULS(20)specificTranferSyntax(3)···}

其余字段的值是相同的,在通常的 ASN.1 编码规则情况下,这些值的前缀均为:

{joint-iso-itu-t asn1(1)···}

注:例如,客体标识符 {joint-iso-itu-t genericULS(20)specificTranfer Syntax(3)ber(1)} 约定采用基本编码规则,而客体标识符 {joint-iso-ccittgenericULS(20)specificTranferSyntax(3)ber-derived(2)distinguished-encoding(1)} 则约定采用区分编码规则。

10 一致性

声称与本部分一致的系统,当使用由 ASN.1 客体标识符对第 6 章中给出的“GenericProtecting TransferSyntax”模块标识的保护传送语法时,应支持合适的 ASN.1 以及任何相关的约定。

目 次

前言	III
ISO/IEC 前言	IV
引言	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 一般概述	2
6 保护传送语法用的数据结构	4
7 与下层协议合用	5
8 同步规程	5
9 客体标识符分配	6
10 一致性	6

c) 在保护表示上下文中的连续 PDV。

6 保护传送语法用的数据结构

保护传送语法使用的一组数据结构由下列 ASN.1 模型中的 ASN.1 类型 SyntaxStructure 定义。该 SyntaxStructure 类型由客体集 ValidSTs(它是 SECURITY-TRANSFORMATION 客体的结合)进行参数化。当提供了 ValidSTs 的值,以及相应的安全变换规范时,SyntaxStructure 类型就变成成为具体保护传送语法的一个完整语法规范。

```
GenericProtectingTransferSyntax{joint-iso-ccitt genericULS(20)
  modules(1) genericProtectingTransferSyntax(7)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS
  SyntaxStructure{};
IMPORTS
  notation
    FROM ObjectIdentifiers{joint-iso-ccitt
      genericULS(20) modules(1) objectIdentifiers(0)}
  SECURITY-TRANSFORMATION, ExternalSAID
    FROM Notation notation;
SyntaxStructure{SECURITY-TRANSFORMATION; ValidSTs} ::= CHOICE
{
  firstPdvExplicit FirstPdvExplicit{{ValidSTs}},
  ——用于表示上下文结合或单项结合安全联系情况下的,
  ——保护表示上下文的第一个 PDV 或
  ——除表示上下文之外发送的要保护 PDV。
  firstPdvExternal FirstPdvExternal{{ValidSTs}},
  ——用于外部建立安全联系情况下的,
  ——保护表示上下文的第一个 PDV 或
  ——除表示上下文之外发送的要保护 PDV。

  subsequentPdv SubsequentPdv{{ValidSTs}}
  ——用于保护表示上下文中的连续 PDV。
}
FirstPdvExplicit {SECURITY-TRANSFORMATION; ValidSTs} ::= SEQUENCE
{
  transformationId SECURITY-TRANSFORMATION. &sT-Identifier
    ({{ValidSTs}}),
  staticUnprotParm
    SECURITY-TRANSFORMATION. &StaticUnprotectedParm
    ({{ValidSTs}}{@transformationId})
  OPTIONAL,
```

前 言

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。

本部分为 GB/T 18237 的第 4 部分,本部分等同采用国际标准 ISO/IEC 11586-4:1996《信息技术 开放系统互连 通用高层安全:保护传送语法规范》(英文版)。

本部分由中华人民共和国信息产业部提出。

本部分由中国电子技术标准化研究所(CESI)归口。

本部分起草单位:中国电子技术标准化研究所(CESI)。

本部分主要起草人:郑洪仁。