ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 18237.1—2000
idt ISO/IEC 11586-1:1996

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

Information technology—Open Systems Interconnection—Generic upper layers security—Part 1:Overview,models and notation

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 11586-1:1996《信息技术　开放系统互连　通用高层安全:概述、模型和记法》。

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

本标准的附录 A 到附录 F 是标准的附录。

本标准的附录 G 到附录 J 是提示的附录。

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 11586-1 是由 ISO/IEC JTC 1"信息技术"联合技术委员会的 SC21"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.830。

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 到附录 F 构成为本标准的一部分。附录 G 到附录 J 仅提供参考信息。

引　　言

本标准是系列标准的一部分，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 1 部分。

在本系列标准中描述的全部设施的应用方面的信息指南见附录 G。

重要的是要注意到，一般安全设施本身不提供安全服务；它们只是与安全有关的协议的构造工具。而且，这些设施并不是必需给应用的全部安全通信需求提供独立解释。应用标准仍需要在其规范内体现安全特征，以便与通用高层安全设施提供的通用安全服务一起工作。

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1部分:概述、模型和记法

GB/T 18237.1—2000
idt ISO/IEC 11586-1:1996

Information technology—Open Systems Interconnection—Generic upper layers security—Part 1:Overview,models and notation

1　范围

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

a)　一组记法工具,这组工具支持抽象语法规范中的选择字段保护需求的规范,并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　本标准定义了如下内容:

a)　基于OSI高层安全模型(GB/T 17965)中描述的概念的安全交换协议功能和安全变换的通用模型;

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

c)　由本系列标准包含的通用高层安全设施的应用方面的一组信息性指南。

1.3　本标准没有定义如下内容:

a)　可能由其他标准要求的一组完备的高层安全设施;

b)　适于特定应用的一组完备的安全设施;

c)　用作支持安全服务的机制。

1.4　安全交换模型和支持记法既打算用作为定义本系列标准所属各部分中的安全交换服务元素的基础,又用于欲将安全交换引入到其自身规范的任何其他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 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(idt ISO/IEC 7498-1:1994)

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分:安全体系结构(idt ISO/IEC 7498-2:1989)

GB/T 12453—1990　信息处理系统　开放系统互连　运输服务定义(idt ISO/IEC 8072:1986)

GB/T 15695—1995　信息处理系统　开放系统互连　面向连接的表示服务定义

国家质量技术监督局2000-10-17批准　　2001-08-01实施

(idt ISO/IEC 8822:1988)

GB/T 15696—1995 **信息处理系统 开放系统互连 面向连接的表示协议规范** (idt ISO/IEC 8823:1988)

GB/T 16264.3—1996 **信息技术 开放系统互连 目录 第3部分:抽象服务定义** (idt ISO/IEC 9594-3:1990)

GB/T 16264.8—1996 **信息技术 开放系统互连 目录 第8部分:鉴别框架** (idt ISO/IEC 9594-8:1990)

GB/T 16688—1996 **信息处理系统 开放系统互连 联系控制服务元素协议规范** (idt ISO/IEC 8649:1988)

GB/T 17176—1997 **信息技术 开放系统互连 应用层结构**(idt ISO/IEC 9545:1994)

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 17969.1—2000 **信息技术 开放系统互连** OSI **登记机构的操作规程 第**1 **部分:一般规程**(idt ISO/IEC 9834-1:1993)

ISO/IEC 8824-1:1995 **信息技术 抽象语法记法** 1(ASN.1):**基本记法规范**

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 8824-3:1995 **信息技术 抽象语法记法** 1(ASN.1):**约束规范**

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**

ISO/IEC 8825-1:1995 **信息技术** ASN.1 **编码规则:基本编码规则**(BER)、**典型编码规则**(CER)**和区分编码规则**(DER)**规范**

ISO/IEC 10181-2:1996 **信息技术 开放系统互连 开放系统安全框架:鉴别框架**

ISO/IEC 10181-3:1996 **信息技术 开放系统互连 开放系统安全框架:访问控制框架**

3 定义

3.1 **本标准采用** GB/T 9387.1 **中定义的下列术语:**

——**传送语法** transfer syntax。

3.2 **本标准采用** GB/T 9387.2 **中定义的下列术语:**

——**访问控制** access control;

——**机密性** confidentiality;

——**数据源鉴别** data origin authentication;

——**解密** decipherment;

——**数字签名** digital signature;

——**加密** encipherment;

——**完整性** integrity;

——**密钥** key;

——**密钥管理** key management;

——**选择字段保护** selective field protection。

3.3 **本标准采用** GB/T 15695 **中定义的下列术语:**

——**抽象语法** abstract syntax;

——**表示上下文** presentation context;

——**表示数据值** presentation data value。

3.4 **本标准采用** GB/T 17176 **中定义的下列术语:**

——**应用联系** application-association;

——**应用上下文** application-context;

——**应用服务元表**(ASE) application-service-element(ASE)。

——**应用服务客体联系**(ASO 联系) application-service-association(ASO-association);

3.5 **本标准采用** ISO/IEC 10181-2 **中定义的下列术语**:

——**鉴别交换** authentication exchange;

——**请求者** claimant;

——**实体鉴别** entity authentication;

——**验证者** verifier。

3.6 **本标准采用** ISO/IEC 10181-3 **中定义的下列术语**:

——**访问控制证书** access control certificate。

3.7 **本标准采用** GB/T 17965 **中定义的下列术语**:

——**安全联系** security association

——**安全通信功能**(SCF) security communication function(SCF)

——**安全交换** security exchange

——**安全交换项** security exchange item

——**安全交换功能** security exchange function

——**安全变换** security transformation

——**系统安全客体**(SSO) system security object (SSO)

3.8 **本标准采用下列定义**:

3.8.1 **表示上下文结合安全联系** presentation context-bound security association

一种安全联系,同保护表示上下文一起建立,它用于该保护表示上下文中向一个方向发送的全部表示数据值;这种安全联系的属性与保护表示上下文中第一个表示数据值的编码一起被显式地指出。

3.8.2 **单项结合安全联系** single-item-bound security association

一种安全联系,它用于与表示上下文无关的单个独立保护的表示数据值;这种安全联系的属性与表示数据值编码一起被显式地指出。

3.8.3 **外部建立的安全联系** externally-established security association

一种安全联系,它是不依赖于其使用实例建立的,并具有使其能在使用时被引用的全局唯一性的标识符。

3.8.4 **初始编码规则** initial encoding rules

当 ASN.1 **类型值使用安全变换进行保护时,用于从** ASN.1 **类型的值生成无保护位串的** ASN.1 **编码规则。**

3.8.5 **保护表示上下文** protecting presentation context

使保护传送语法和抽象语法相联系的表示上下文。

3.8.6 **保护传送语法** protecting transfer syntax

使用安全变换的传送语法。

3.8.7 **保护映射** protection mapping

使由抽象语法规范中的名字标识的保护需求与为满足这种需求欲使用的具体安全变换相关联起的规范。

4 缩略语

ACSE **联系控制服务元素**

ASE **应用服务元素**

ASO **应用服务客体**

GULS **通用高层安全**

OSI 开放系统互连
PDU 协议数据单元
PDV 表示数据值
PICS 协议实现一致性声明
SCF 安全通信功能
SEI 安全交换项
SESE 安全交换服务元素
SSO 系统安全客体

5 一般概述

通用高层安全(GULS)标准定义了一组用于支持提供适于多种应用的安全保护的协议构造工具和协议成分。这些设施支持 OSI 高层(应用层,有时连同表示层的支持)中提供的安全服务。

注:可以在高层或低层用安全机制为 OSI 应用提供安全服务。在低层情况下,这种保护通过在建立应用联系时规定相应的 ACSE 保护服务质量(在 GB/T 12453 中定义)获得。这种保护服务质量通过表示层和会话层透明地传给运输服务。低层中提供的安全服务不在本标准范围之内。

在 GULS 标准中提供的设施包括:

——构建用于支持在成对通信的应用实体调用之间交换安全相关信息的应用层协议成分的通用手段(由 SESE 支持的安全交换概念);这些设施在第 6 章中描述;

——为保护信息项而使用表示层设施执行信息项上的安全相关变换的通用方法(由一般保护传送语法支持的安全变换概念);这些设施在第 7 章中描述;

——抽象语法记法工具,以便对应用协议的设计者在规定用于这种协议可选字段(PROTECTED 参数化类型,以及这种类型的 PROTECTED-Q 变量)的安全保护时有所帮助;这些设施在第 8 章中描述。

安全交换被用作实体鉴别和密钥管理目的。安全变换(以及通用保护传送语法和/或 PROTECTED 参数化类型或其变种)被用作完整性、机密性、数据源鉴别和/或抗抵赖目的。

高层安全模型(GB/T 17965)为 GULS 规范提供了一个体系结构模型。它描述了安全交换功能和安全变换的作用。

安全交换功能为作为安全机制操作一部分的应用实体调用之间的安全信息交流提供了手段,即它们生成和处理与安全相关目的的应用协议控制信息。安全交换可以用本标准中的记法规定,然后可引入任何抽象语法规范。安全交换服务元素(SESE)是一种 GB/T 18237.2 和 GB/T 18237.3 中定义的应用服务元素(ASE)。SESE 提供了运送安全交换的途径,它支持生成与所用安全机制无关的应用特定的 ASE 的目标。然而,直接体现安全条款的应用规范的某些内容应依赖机制。

安全变换由 GB/T 18237.4 中描述的通用保护传送语法支持。

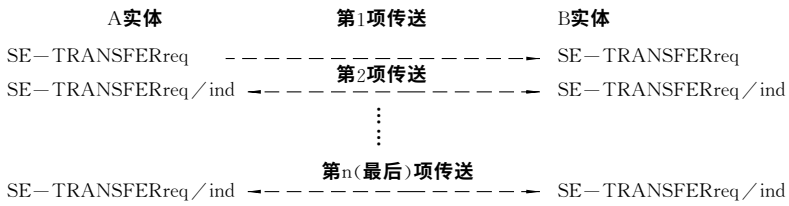
6 安全交换

6.1 安全交换模型

本标准定义了 GB/T 17965 中介绍的安全交换规程模型。

安全交换发生在 A 和 B 两个实体之间。它包含一个从 A 传送到 B 的安全交换项,可能后随 A 和 B 之间以任一方向传送的一个或多个 SEI 的序列。传送的个数取决于特定的安全交换。每一个 SEI 可由用任意 ASN.1 类型表示的任意复合数据结构构成。它可包括使用第 8 章中描述的 PROTECTED 记法单个保护的若干成分。

图 1 中的时序图说明了用于 n 次安全交换的 SEI 传送序列,以及在 GB/T 18237.2 中定义的相应 SESE 服务原语调用。



注：双向箭头指出该传送可由 A 或 B 发送。

图 1　安全交换模型

存在以下两类交换：

——交替的：在交替的方向上进行的连续的项传送，并且在任何时刻仅有一个传送有效；

——任意的：对任何传送的方向都不加限制，并且在两个方向的传送都可以同时有效。

当安全交换正在进行时，其他信息传送也可以进行，并且其他安全交换可以在同一个应用联系上进行。然而，应用上下文规则通常会限制这类重叠活动。运送 SEI 的表示数据值可以同其他表示数据值拼接、交错，或嵌入其他表示数据值中。

6.2　规定安全交换用的记法

安全交换的规范包括可被交换的 SEI 的类型的规范、用于这些 SEI 的传送的次序限制的声明、可由每个 SEI 的传送造成的差错条件的声明，以及相关语义(或引用相关语义)的声明。

安全交换定义包括：

a) 分配给安全交换的全局客体标识符或局部整数值，以便使其使用在协议中被无二义性地进行标识；

b) SEI 的抽象语法规范和安全交换中传送的差错通知。

为了支持以 SESE 协议能使用的形式表示的信息的规范，因而提供了以下三种 ASN.1 信息客体类定义(见 ISO/IEC 8824.2)。

——SECURITY-EXCHANGE 信息客体类用于规定特定的安全交换；这类信息客体包含一个或多个 SEC-EXCHG-ITEM 信息客体；

——SEC-EXCHG-ITEM 信息客体类用于定义一个 SEI；这类信息客体可以包含一个或多个 ERROR 信息客体；

——SEC-ERROR 信息客体类用来定义可由 SEI 的传送造成的差错条件。

注：附录 G 中提供了如何在完整的应用上下文中使用这些信息客体类的指南。

```
SECURITY-EXCHANGE::=CLASS
--这个信息客体类定义用于规定安全交换的特定实例。
    {
    &SE-Items       SEC-EXCHG-ITEM,
    --这是 ASN.1 信息客体的集合，由一组安全交换项构成。
    &sE-Identifier      Identifier      UNIQUE
    --用于特定安全交换的局部或全局标识符
    }
    WITH SYNTAX
    --下列语法用于规定特定安全交换。
    {
      SE-ITEMS      &SE-Items
      IDENTIFIER      &sE-Identifier
    }
    Identifier::=CHOICE
```

```
{
  local      INTEGER,
  global     OBJECT IDENTIFIER
}
SEC-EXCHG-ITEM::=CLASS
{
  &Item Type,
  --用于本交换项的 ASN.1 类型。
  &itemId      INTEGER,
  --用于本项的标识符,例如 1、2、3……。
  &Errors      SE-ERROR      OPTIONAL
  --由本项的传送造成的差错可选列表。
}
WITH SYNTAX
{
  ITEM-TYPE      &ItemType
  ITEM-ID        &itemId
  [ERRORS      &Errors]
}
SE-ERROR::=CLASS
{
  &ParameterType      OPTIONAL,
  --与返送给 SEI 发送者的差错条件通知相伴的参数的 ASN.1 类型。
  &errorCode      Identifier UNIQUE
  --用于将差错条件返送给 SEI 发送者的标识符
}
WITH      SYNTAX
}
  [PARAMETER   &Parameter-Type]
  ERROR-CODE   &errorCode
}
```

使用本记法的例子在附录 C 中给出。

7 安全变换

7.1 安全变换模型

安全变换是为保护通信或存储期间的用户数据而施用于用户数据的安全函数(或安全函数的组合)。安全变换包含通信或存储前施用的编码过程,以及收到或检索时可(但不必总是)用的解码过程。安全变换的例子有:

a) 在数据编码时应用一个加密过程和解码时应用一个对相的应解密过程。

b) 在编码时生成密封或签名,并将其附加到数据上;在解码时检查和去除附加的密封或签名;

c) 将 a)和 b)中的函数组合成为一种安全变换。

使用 7.2 中的记法定义的安全变换适用于 OSI 应用(连同 GB/T 18237.4 中定义的一般保护传送语法)或其他目的,包括局部存储和非 OSI 通信时的脱机保护。

注：7.1.5 描述了安全变换在 OSI 表示连接上的使用。7.1.6 描述了其与 OSI 表示协议无关的使用。

安全变换可以构成提供安全服务(例如机密性、完整性、数据源鉴别)的主要手段，或者他们有助于提供安全服务(例如实体鉴别、访问控制、抗抵赖)。

图 2 说明了对于传送或存储时的保护数据项中包含的步骤。

在编码系统中，导出未保护数据项的变换(被保护)表示的过程是：

a) 如果未保护项是如抽象语法记法中规定的 ASN.1 类型的值，则使用初始编码规则对位串表示进行编码；然后

b) 将安全变换的编码过程用于未保护项的位串表示，也可使用附加的本地输入信息，以获得已变换的项，它是 ASN.1 类型 XformedDataType(该精确类型被指定为安全变换定义的一部分)的值；然后

c) 对由 b)产生的 ASN.1 值进行编码(也许是构成 ASN.1 值的编码过程的一部分，诸如 GB/T 18237.4 中定义的保护传送语法结构)。

在解码系统中，恢复未保护数据项和/或对安全泄露进行检查的过程是：

d) 对收到的或检索到的已变换项进行解码，这种项是类型 XformedDataType 的 ASN.1 值(这种解码过程可以形成构成 ASN.1 值解码的一部分，诸如 GB/T 18237.4 中定义的保护传送语法结构)；然后

e) 将安全变换的解码过程用于收到或检索到的值，也可使用附加的本地输入信息，并根据那种解码过程产生输出(依据特定的变换，输出可以包括已恢复的未保护项的拷贝、签名或密封验证成功/失败的指示，和/或局部存储作为今后使用的签名的拷贝)；然后

f) 如果步骤 e)的输出是已恢复的未保护项的拷贝，并且如果那个项是抽象语法记法中规定的 ASN.1 类型的值，则使用与步骤 a)相同的初始编码规则对那个数据项解码。

步骤 a)和 f)中的初始编码规则的确定在 7.1.4 中描述。注意，安全变换通常可能操作在数据项而不是 ASN.1 类型的值(例如任意位串)，所以这种编码过程未必总是需要的。

步骤 c)和 d)的编码规则的确定应取决于存储或通信环境，而不取决于所使用的特定安全变换。

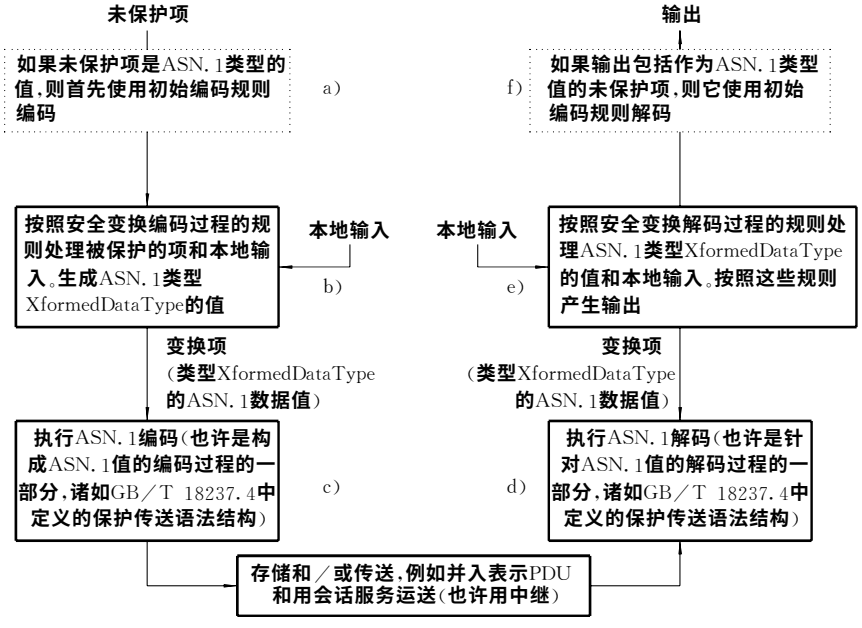


图 2 数据项的保护存储或传送

7.1.1 安全变换在 OSI 高层中的体系定位

安全变换在两个或多个系统之间的安全联系上下文中操作。在每一个系统中都有支持这种安全联系的系统安全客体(SSO)。这些 SSO 执行安全变换编码/解码过程(例如加密、数字签名的生成/验证)，并存储必要的安全状态信息(例如密钥、算法、参数、链接状态)。这种 SSO 的内部行为由特定的安全变

换规范以及支持规范，例如算法（它超出了本标准的范围）决定。根据图2，在框b）和e）中指出的功能以SSO为模型。

在编码和解码系统的表示实体中还有安全通信功能（SCF）。这些SCF支持SSO的通信需求。根据图2，在框a）、c）、d）和f）中指出的功能以SCF为模型。SCF行为的定义在本标准的第8章和GB/T 18237.4中给出。

7.1.2 安全联系

安全变换可以反复用于逻辑上有序的数据值序列，例如在两个系统之间以一个方向顺序地传送的表示数据值。相同的保护用于每一个数据值。安全变换对那种序列的应用由安全联系决定。一个以上的安全联系可以同时存在于在一对系统之间，典型情况是提供不同类型的保护。

本标准涉及与高层通信或信息存储相关的安全联系的几个方面。从OSI高层角度看，安全联系是ASO联系的一种形式。

本标准给出以下三种安全联系：

a）外部建立安全联系——一种安全联系，其建立与其使用的实例无关，并且具有能使它在使用时引用的全局唯一性的标识符。建立这种安全联系的方法不在本标准中规定，而且它的生存期不受本标准限制。外部建立的安全联系的标识符包括一个整数值，以及分配那个整数值的系统身份。（这个身份可能是隐式已知的，例如发送者或接收者，因此，这个身份并不是总要在协议中出现。）

b）单项结合安全联系——用于单一独立保护表示数据值的一种安全联系，它与表示上下文没有联系；安全联系的属性与表示数据值编码一起被显式指出。单项结合安全联系的生存期受表示数据值生存期限制。

c）表示上下文结合安全联系——一种安全联系，它与保护表示上下文的建立一起建立，并且用于那个保护表示上下文中某一方向发送的全部表示数据值集；安全联系的属性与保护表示上下文中的第一个表示数据值编码一起被显式指出。只有当保护与使用的OSI表示服务和协议（分别在GB/T 15695和GB/T 15696中规定）一起提供时，这种安全联系类型才能适用。这种安全联系的生存期与相应保护表示上下文的生存期相同。

安全变换的施行可由本地安全状态信息和/或由已编码数据值传送或存储的参数决定。在一个安全联系内，本地安全状态信息可以从安全变换的一次应用保持到它的下一次应用。例如，对于提供安全联系内表示数据值序列完整性的变换，诸如完整性序列号或密码链接值之类的状态信息应从变换的一次应用保留到下一次应用。静态参数的值（见7.1.3）也保留在整个安全联系内。

7.1.3 安全变换参数

当使用安全变换时，参数值以及已变换的数据值需要在编码和解码函数之间运送。参数具有以下两种类型：

a）静态参数——这些参数在整个安全联系内都保持常数值，而且安全变换在安全联系中第一次应用时或应用前，这些参数要由数据的编码者予以规定；

b）动态参数——当变换在安全联系的使用过程中，这些参数可以动态地改变；由数据的编码者指出数据流内的那些变化。

静态参数的例子是：

——在安全变换中使用的算法标识符；

——如有必要，算法的操作方式；

——与上述提到的算法一起使用的密钥或密钥标识符；

——如有必要，初始化向量的值。

动态参数的例子是在一段使用期后会发生变化的密钥。

参数值可以编码成未保护的，或者它们本身可以要求保护。未保护参数在支持安全变换的保护传送语法的显式字段中运送。保护参数以及被保护的值被当作安全变换编码过程的输入。在安全变换规则

中必须规定这些参数是如何表示的，它们的表示是如何与已编码的抽象语法规则结合的，并且如何使这种结果生成传送或存储用的 ASN.1 数据值。

注：作为运送被保护参数的一个例子，见第 D4 章中 GULS SIGNED 安全变换的定义。

安全变换所要求的参数数据（例如密钥）也可以由其他方法获得，包括：

——更早的应用层协议交换（例如由 SESE 运送的密钥推导安全交换）；

——本地方法（例如密钥的人工插入）。

7.1.4 初始编码规则的确定

以图 2 中框 a）和 f）为模型的初始编码（和最终解码）过程的规则以下列方法之一确定：

a）安全变换可以提供作为安全变换（被保护或未被保护的）静态参数的初始编码规则的指示运送；

b）作为缺省，每个安全变换规范都要确定缺省初始编码规则。

注：当数字签名用于抗抵赖时，被变换项（即已签名的数据）可能需要存储在接收方系统中，和/或中继给其他实体。在这种情况下，计算签名时使用的初始编码规则知识必须保留。对于数字签名，建议使用安全变换规范中确定的缺省编码规则。于是，所要求的知识能够通过存储/转换安全变换标识符和签名保留。

7.1.5 OSI 表示连接上安全变换的用法

OSI 表示层将传送语法与所使用的每个抽象语法相联系。当使用安全变换时，传送语法就代表保护传送语法。

按照 ISO/IEC 8824，表示数据值可以在下述两种情况之一传送：

a）在已协商的表示上下文内；

b）（作为使用 ASN.1 EXTERNAL 或 EMBEDDED PDV 记法时的选项）在表示上下文之外。

在这两种情况下，被保护的表示数据值用保护传送语法表示。GB/T 18237.4 所定义的保护传送语法支持静态和动态安全变换参数的通信。

上述 a）包括保护表示上下文。在保护表示上下文内沿一个方向传送的全部表示数据值都使用相同的安全变换来保护，并由一种安全联系来控制。当保护表示上下文建立时（使用 GB/T 15695 和 GB/T 15696中规定的建立表示上下文的规程），则在这种表示上下文的每个方向上的第一个表示数据值应是下列之一：

a）引用外部建立的安全联系；

b）定义新的表示上下文结合安全联系。

当表示数据值在表示上下文之外被编码时，则表示数据值应是下列之一：

a）引用外部建立的安全联系；

b）定义新的单项结合安全联系。

在 OSI 表示连接上，不同的安全联系用于每个流向。这些安全联系可使用相同的安全变换，但并不要求这样做。

注：上述限制（即当使用 OSI 表示协议时，不同的安全联系用于每一个流向）确保了在两个不同流向之间没有共享的公共密码状态变量。如果这种共享的状态能存在，则需要一种处理诸如会话层重新同步一类事件的表示层中复杂的状态维护协议元素。实际上，两个方向分开的安全联系很可能具有从一个包含安全联系中派生出来的共同属性。

7.1.6 与 OSI 表示协议无关的安全变换的用法

安全变换可以独立于 OSI 表示协议使用，例如用于存储保护。在 7.1.2 至 7.1.5 中描述的概念和规程施用时具有下列限制。

全部被保护表示数据值都在表示上下文之外表示。

可以使用单项结合安全联系或外部建立的安全联系。不能用表示上下文结合安全联系。在被保护信息未被交换，但仅对由始发者的使用予以保护的地方，则安全变换也可以在没有安全联系时使用。

如果使用外部建立的安全联系，则外部建立的安全联系的生存期必须复盖被保护数据的存储生存期。

7.2 规定安全变换用的记法

安全变换规范包括需由保护传送语法结构识别的数据项的规范。为此，提供了下列 ASN.1 信息客体类定义(见 ISO/IEC 8824-2)：

```
SECURITY-TRANSFORMATION::=CLASS
--这个信息客体类定义在规定安全变换的特定实例时使用。
{
&sT-Identifier      OBJECT IDENTIFIER UNIQUE,
--用未指示特定安全变换应用的标识符。
&initialEncodingRules OBJECT IDENTIFIER,
  DEFAULT{joint-iso-ccitt asnl(1) ber-derived(2)
  canonical-encoding(0))},
--在用安全变换的编码过程之前
--用于生成位串的缺省初始编码规则。
&StaticUnprotectedParm OPTIONAL,
--用于运送静态未保护参数的 ASN.1 类型。
&DynamicUnprotectedParm OPTIONAL,
--用于运送动态未保护参数的 ASN.1 类型。
&XformedDataType,
--由安全变换编码过程产生的
--ASN.1 值的 ASN.1 类型。
&QualifierType OPTIONAL
--&QualifierType 规定与 PROTECTED-Q 记法
--一起使用的限定符参数的 ASN.1 类型。
WITH SYNTAX
--下列语法用来规定特定的安全变换
{
IDENTIFIER                  &sT-Identifier
[INITIAL-ENCODING-RULES     &initialEncodingRules]
[STATIC-UNPROT-PARM         &StaticUnprotectedParm]
[DYNAMIC-UNPROT-PARM        &DynamicUnprotectedParm]
XFORMED-DATA-TYPE           &XformedDataType
[QUALIFIER-TYPE             &QualifierType]
}
```

使用这种记法的例子在附录 D 中给出。

安全变换规范还需要规定下列细节(尽管在本标准中没有提供支持这种规范的正式记法)：

——编码过程：在编码端，一种变换过程的描述，该过程用于未保护项和被传送的保护参数，以生成最终的变换值(它是类型 &XformedDataType 的 ASN.1 值)。

——编码过程本地输入：本地衍生的输入到编码过程的列表。

——解码过程：在解码端，一种变换过程的描述，该过程用于接收到的或检索到的变换值(它具有类型 &XformedDataType)，以生成未保护数据位串(若有的话)和被传送的保护参数的值。

——解码过程本地输入：本地衍生的输入到解码过程的列表。

——解码过程输出：解码过程输出的列表(可以包括，也可以不包括未保护项的已被复原的值)。

——参数：全部参数的语义含义、参数的缺省值，以及动态参数应发生变化情况的描述。

——变换限定符：用于这种变换的、调用者指定变换限定符的规则描述。

——差错：在解码过程中可以检测到的差错条件的描述。

8 选择字段保护用的抽象语法记法

下面的抽象语法记法用于选定的 ASN.1 数据类型的抽象保护需求规范。所要求的保护被映射到提供(在抽象级)要求的保护形式的安全变换集之一。某些安全变换接受输入限定符以控制所要求保护的操作，例如，对于用于保护的安全联系的标识符。对于这些情况，要定义基本记法的扩充，以便能由记法的用户来规定限定符。

本章规定：

a) 基本保护抽象语法记法，它用来规定抽象语法规范中所选字段的抽象保护需求；

b) 限定的保护抽象语法记法，它用来规定抽象语法规范中所选字段的抽象保护需求以及相关的限定符；

c) 保护映射记法，它用来规定提供所需保护的一个或多个安全变换的可能映射。

8.1 基本记法

为了帮助抽象语法的编制者指定选择字段保护需求，定义了下列 ASN.1 参数化类型(见 ISO/IEC 8824-4)：

```
PROTECTED{BaseType,PROTECTION-MAPPING:protectionReqd}::=
CHOICE
{
  dirEncrypt BIT STRING (CONSTRAINED BY{BaseType
    --dirEncrypt 只能与 dirEncryptedTransformation 一起使用，
    --并生成像 GB/T 16264.8 ENCRYPTED 类型一样的编码--}),
  dirSign   SEQUENCE
    {
      baseType BaseType OPTIONAL，
       --在 dirSignedTransformation 中必须出现，
       --并且在 dirSignatureTransformation 必须省略
    algorithmId AlgorithmIdentifier，
    encipheredHash BIT STRING (CONSTRAINED BY
       {BaseType--包含 BaseType 值的已加密散列--})
    }
       --dirSign 只能与 dirSignedTransformation 或
       --dirSignatureTransformation 一起使用，
       --并生成像相应 GB/T 16264.8 SIGNED 或 SIGNATURE 一样的编码，
noTransform[0]Base Type，
       --noTransform 表示没有安全变换。
       --受安全策略的影响，如果适当的保护由低层提供，
       --并且数据可以通过的任何应用中继对于维护所要求的
       --保护是可信的，则可使用 noTransform。
       --只有在 protectionReqd.&bypassPermitted 为 TRUE 时
       --才能使用这个选择方式，
direct [1]SyntaxStructure
```

```
        {{protectionReqd.&SecurityTransformation}},
         --direct 产生保护传送语法值,
         --它使用类似 ASN.1 的相同编码规则来编码
         --(类型 SyntaxStructure 引自 GB/T 18237.4),
    embedded [2]EMBEDDED PDV(WITH COMPONENTS{
            identification (WITH COMPONENTS{
                presentation-context-id,
                context-negotiation(WITH COMPONENTS{
                    transfer-syntax(CONSTRAINED BY
                      {OBJECT IDENTIFIER:
                      protectionReqd.&protTransferSyntax})}),
            transfer-syntax(CONSTRAINED BY
                      {OBJECT IDENTIFIER;
                      protectionReqd.&protTransferSyntax})}),
        data-value(WITH COMPONENTS{notation(BaseType)})
        --该编码的数值是类型 BaseType 的值
        })
    }
    --BaseType 是被保护的类型,并且 protectionReqd 是
    --PROTECTION-MAPPING 类的 ASN.1 客体。
    --使用的 PROTECTED 要引入到 PROTECTED 参数化类型
    --以及必要的 PROTECTION-MAPPING 客体定义的用户模块。
```

PROTECTION-MAPPING 客体类以及其含义在 8.3 中描述。对于"protectionReqd"允许的客体的集合在不同的抽象语法规范中是不同的,它依所要求的不同变换的范围而定。从 PROTECTION-MAPPING 客体到变换的映射应包含在 PROTECTION-MAPPING 客体定义集合中。该集合的定义可以在不依赖于(机制独立的)抽象语法规范和(应用独立的)变换定义的 ASN.1 模块中规定。

CHOICE 中的各种选择方式可用于下列不同情况:

——dirEncrypt 和 dirSign:这些选择方式生成所用安全变换的 &XformedDataType。这些选择方式可用来提供某种手段,PROTECTED 记法能利用这种手段生成 GB/T 16264.8 中规定的 ENCRYPTED、SIGNED 和 SIGNATURE 参数化类型的相同位编码。

—— noTransform:这种选择方式不使用安全变换。如果使用的保护映射(见 8.3 和 8.4)指示 &bypassPermitted=TRUE,则它就是允许的。该项以其未保护形式编码。按照安全策略,如果适当的保护由低层提供,并且数据可以通过的任何应用中继对于维护所要求的保护是可信的,则可使用 noTransform。

——direct:按照 GB/T 18237.4 的规定,这种选择方式保护将传送语法值直接引入到所包含的 ASN.1 规范中。它支持使用外部建立的安全联系或单项结合安全联系。它不允许使用已协商的表示上下文。对于保护传送语法结构[以 7.1 中图 2 的框 c)和 d)为模型]编码所使用的编码规则必须与包含 PROTECTED 记法的 ASN.1 类型所使用的规则相同。

——embedded:这个选择方式提供了最大的灵活性,包括将保护与已协商表示上下文相关联的能力以及对 ISO/IEC 11586-4 中定义的已协商表示上下文使用不同保护传送语法的能力。

注:建议按如下选择使用的这些选项:

a) 如果不用 b)、c)或 d),则用直接选项;