ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 18794.1—2002

目　　次

前　　言

本标准等同采用国际标准 ISO/IEC 10181-1:1996《信息技术　开放系统互连　开放系统安全框架:概述》。

GB/T 18794 在《信息技术　开放系统互连　开放系统安全框架》总标题下,目前包括以下几个部分:

第 1 部分(即 GB/T 18794.1):概述

第 2 部分(即 GB/T 18794.2):鉴别框架

本标准的附录 A、附录 B 都是提示的附录。

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:信息产业部电子第十五研究所。

本标准主要起草人:郑磊、张莺、周珍妮。

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(它们都是 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 JTC1。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 10181-1 是由 ISO/IECJTCI"信息技术"联合技术委员会的 SC21"开放系统互连、数据管理和开发分布式处理"分技术委员会与 ITU-T 共同制定的。等同文本为 X.810。

ISO/IEC 10181 在《信息技术　开放系统互连　开放系统安全框架》总标题下,目前包括以下七个部分:

——第 1 部分:概述
——第 2 部分:鉴别框架
——第 3 部分:访问控制框架
——第 4 部分:抗抵赖框架
——第 5 部分:保密性框架
——第 6 部分:完整性框架
——第 7 部分:安全审计和告警框架

本标准的附录 A 和附录 B 仅提供参考信息。

引　　言

很多应用具有安全需求以防范信息通信中遇到的威胁。一些共识的威胁及对付这些威胁可以使用的安全服务和机制在GB/T 9387.2中描述。

本标准定义了开放系统安全服务中的框架。

中华人民共和国国家标准

信息技术　开放系统互连　开放系统安全框架　第1部分：概述

GB/T 18794.1—2002
idt ISO/IEC 10181-1:1996

Information technology—Open Systems Interconnection—Security frameworks for open systems—Part 1:Overview

1　范围

安全框架涉及在开放系统环境中安全服务的应用，其中术语“开放系统”系指包括诸如数据库、分布式应用、ODP 和 OSI 一类的领域。安全框架主要用来提供在系统内和系统间交互时对系统和客体的保护方法。安全框架不考虑用于构造系统或者机制的方法学。

安全框架涉及用于获取具体安全服务所使用的数据元素和操作序列（但不是协议元素）。这些安全服务可适用于系统的通信实体，也可以用于系统间交换的数据和由系统管理的数据。

安全框架提供了进一步标准化的基础，对特定安全需求的通用抽象服务接口提供了一致性的术语和定义。安全框架还对能够用于实现这些需求的机制进行了分类。

一种安全服务经常依赖于其他的安全服务，使得安全的一部分与其他的部分进行隔离很困难。安全框架述及特定的安全服务，描述能够用于提供这些安全服务的机制范围，并标识这些服务和机制间的相互关系。这些机制的描述可能涉及对不同安全服务的依赖关系，安全框架用此方式描述一个安全服务对另一个安全服务的依赖关系。

安全框架的本部分包括：

——描述安全框架的整体组织；

——定义多个安全框架中所需要的安全概念；

——描述在框架的其他部分中所标识的服务和机制间的相互关系。

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）

3　术语和定义

下列术语和定义可用于本概述或安全框架的其他部分。

3.1　基本参考模型定义

本标准采用 GB/T 9387.1 中定义的下列术语：

——(N)层(N)-layer；

中华人民共和国国家质量监督检验检疫总局 2002-07-18 批准　　2002-12-01 实施

——(N)**实体**(N)-entity；

——(N)**协议数据单元**(N)protocol-data-unit；

——**应用进程** application process；

——**实开放系统** real open system；

——**实系统** real system；

3.2 **安全体系结构定义**

本标准采用 GB/T 9387.2 **中定义的下列术语**：

——**访问控制** access control；

——**可用性** availability；

——**密文** ciphertext；

——**密码校验值** cryptographic checkvalue；

——**解密** decipherment；

——**拒绝服务** denial of service；

——**数字签名** digital signature；

——**加密** encipherment；

——**内部威胁** insider threat；

——**密钥** key；

——**密钥管理** key management；

——**明文** plaintext；

——**外部威胁** outsider threat；

——**安全审计** security audit；

——**安全标签** security label；

——**安全政策** security policy；

——**敏感性** sensitivity；

——**威胁** threat；

3.3 **补充定义**

本标准采用下列定义。

3.3.1 **非对称密码算法** asymmetric cryptographic algorithm

在执行加密或与之相应的解密中用于加密和解密的密钥是不相同的算法。

注：使用某些非对称密码算法，密文的解密或数字签名的生成要求使用一个以上的私有密钥。

3.3.2 **证书机构** certification authority

创建包含一类或多类安全相关数据的安全证书的可信实体(在安全政策上下文中)。

3.3.3 **条件可信实体** conditionally trusted entity

在安全政策上下文中的可信实体，但其不能违犯安全政策且未被发现。

3.3.4 **密码编链** cryptographic chaining

用于密码算法的一种方式，其中由算法执行的变换依赖于前一过程的输入或输出的值。

3.3.5 **数字指纹** digital fingerprint

数据项的一种特性，诸如密码校验值或对数据执行单向散列函数的结果，其足以代表数据项的独特性，试图找出拥有相同特性的另一数据项在计算上是不可行的。

3.3.6 **可区分标识符** distinguishing identifier

唯一标识一个实体的数据。

3.3.7 **散列函数** hash function

将一个(可能非常)大量的值映射到较小范围的值的(数学)函数。

3.3.8 **单向函数** one-way function

一种易于计算，但如果知道结果，不可能通过计算找出得到该结果的值的(数学)函数。

3.3.9 **单向散列函数** one-way hash function

一种既是单向函数又是散列函数的(数学)函数。

3.3.10 **私有密钥** private key

在非对称密码算法中使用的并且其拥有者是受限制(通常只能由一个实体拥有)的密钥。

3.3.11 **公开密钥** public key

在非对称密码算法中使用的并且可以被公开的密钥。

3.3.12 **撤消证书** revocation certificate

为表明某个特定的安全证书已经撤消而由某个安全机构颁发的安全证书。

3.3.13 **撤消列表证书** revocation list certificate

用于识别一个已撤消安全证书列表的安全证书。

3.3.14 **封印** seal

一种支持完整性但不能防止由接收者伪造的密码校验值(即它不提供抗抵赖)。当封印与一个数据元素相关联时，该数据元素被称为已被封印。

注：尽管封印自身不提供抗抵赖，但某些抗抵赖机制可以使用封印提供的完整性服务，如用可信第三方保护通信。

3.3.15 **秘密密钥** secret key

用于对称密码算法的密钥。秘密密钥的拥有者是受限制的(通常仅限两个实体)。

3.3.16 **安全管理员** security administrator

负责定义或实施一部分或多部分安全政策的人员。

3.3.17 **安全机构** security authority

负责定义、实现或实施安全政策的实体。

3.3.18 **安全证书** security certificate

由安全机构或可信第三方颁发的一组安全相关的数据和用于为这些数据提供完整性和数据源鉴别服务的安全信息。

注：所有的证书实际都是安全证书(见 GB/T 9387.2 中的相关定义)。安全证书术语的采用是为了避免与 GB/T 16264.8(目录鉴别标准)的术语相冲突。

3.3.19 **安全证书链** security certificate chain

一组有序的安全证书序列，其中的第一个安全证书包含安全相关的信息，每一后续的安全证书包含可用来验证前一个安全证书的安全信息。

3.3.20 **安全域** security domain

由若干元素、一个安全政策、一个安全机构和一组安全相关的活动构成的集合，在其中这组元素受控于适于某些具体活动的安全政策，并且安全政策由安全域的安全机构所管理。

3.3.21 **安全域机构** security domain authority

负责实现安全域中安全政策的安全机构。

3.3.22 **安全信息** security information

实现安全服务所需要的信息。

3.3.23 **安全恢复** security recovery

当发现或怀疑已经发生安全违规时所采用的动作和执行的规程。

3.3.24 **安全交互规则** secure interaction rules

规定安全域间交互的安全政策规则。

3.3.25 **安全政策规则** security policy rules

在实系统中安全域的安全政策的表示法。

3.3.26 **安全权标** security token

在通信实体间被传送的，由一个或多个安全服务保护的一组数据以及提供那些安全服务所使用的安全信息。

3.3.27 **对称密码算法** symmetric cryptographic algorithm

在加密或与之对应的解密中使用相同密钥进行加密和解密的算法。

3.3.28 **信任** trust

当且仅当实体 X 依赖于实体 Y 以特定的方式行事时，实体 X 被称为信任实体 Y 的一组活动。

3.3.29 **可信实体** trusted entity

假设执行了其不会执行的动作，或是未能够成功地执行假设其会执行的动作而违犯安全政策的实体。

3.3.30 **可信第三方** trusted third party

就某些安全相关的活动而言(在安全政策的上下文中)是可信的安全机构或其代理。

3.3.31 **无条件可信实体** unconditionally trusted entity

可违犯安全政策而不被发现的可信实体。

4 缩略语

本标准定义了如下缩略语：

ACI **访问控制信息** (Access Control Information)

OSI **开放系统互连** (Open Systems Interconnection)

ODP **开放分布式处理** (Open Distributed Processing)

SI **安全信息** (Security Information)

TTP **可信第三方** (Trusted Third Party)

5 记法

本标准所使用的层记法与 GB/T 9387.1 定义相同。

如果术语“服务”未做限定，则指安全服务。

如果术语“证书”未做限定，则指安全证书。

6 组织结构

本安全框架是 GB/T 18794 系列标准的一部分。这些安全框架在下面描述。其他的安全框架可能在将来说明。密钥管理框架不是 GB/T 18794 的一部分，但它的范围与本文类似，为完整起见本文也包含对它的描述。

6.1 第 1 部分：概述

见第 1 章。

6.2 第 2 部分：鉴别

本框架描述了提供给开放系统的鉴别的所有方面，并描述了鉴别与其他安全功能如访问控制的关系，鉴别的管理需求等内容。

本框架：

a) **定义鉴别的基本概念；**

b) **确定可能的鉴别机制类；**

c) **定义用于这些鉴别机制类的服务；**

d) **确定为支持这些鉴别机制类的协议的功能需求；**

e) **确定鉴别的通用管理需求。**

鉴别框架是位于提供概念、术语和鉴别方法分类的鉴别标准的层次结构的最顶层。直接位于其下的标准如GB/T 15843(实体鉴别机制)提供了一套对这些方式更详细的特殊说明。在层次结构的最低层,如GB/T 16264.8(目录鉴别框架)等标准在具体应用或需求的上下文中使用这些概念和方法。

鉴别框架描述了鉴别的模型,鉴别活动可被分类成的一些阶段,可信第三方的使用,为交换鉴别信息而使用的鉴别证书,基于这些阶段的通用鉴别服务,以及提供这些通用鉴别服务的至少五类鉴别机制。这些鉴别机制包括防止鉴别信息泄露的机制,在相同(和/或不同)验证者的防泄露和防重发保护机制。

6.3 第3部分:访问控制

本框架描述开放系统中的全部访问控制(如用户到进程,用户到数据,进程到进程,进程到数据),以及与其他安全功能如鉴别和审计的关系和访问控制的管理需求。

本框架:

a) 定义访问控制的基本概念;

b)举例说明用于支持一些公认的访问控制服务和机制的访问控制的基本方式;

c) 定义这些服务和相应的访问控制机制;

d) 确定为支持这些访问控制服务和机制的协议的功能需求;

e) 确定为支持这些访问控制服务和机制的管理需求;

f) 述及访问控制服务和机制与其他安全服务和机制的交互。

本安全框架描述了访问控制的模型,在其中访问控制活动可以分类成的一些阶段,基于这些阶段的通用访问控制服务,以及这些通用访问控制服务的至少三类访问控制机制。这些访问控制机制包括访问控制表、能力和标签。

6.4 第4部分:抗抵赖

本框架细化和扩充了GB/T 9387.2中描述的抗抵赖服务的概念,并且提供了开发和提供这些服务的框架。

本框架:

a) 定义抗抵赖的基本概念;

b) 定义通用抗抵赖服务;

c) 确定提供抗抵赖服务的可能的机制;

d) 确定抗抵赖服务和机制的通用管理需求。

6.5 第5部分:保密性

保密性服务的目的是保护信息免于非授权的泄露。本框架述及在恢复、传送以及管理中的信息保密性。

本框架:

a) 定义保密性的基本概念;

b) 确定可能的保密性机制类;

c) 定义每一类保密性机制的设施;

d) 确定为支持保密性机制类的管理需求;

e) 述及保密性机制和其支撑服务与其他安全服务和机制的相互关系。

在安全框架中描述的某些规程通过密码技术的应用实现保密性。使用本框架不依赖于特定密码或其他算法的使用,尽管某种保密性机制类可能依赖于特定的算法性质。

6.6 第6部分:完整性

数据未被以非授权的方式改变或毁坏的性质被称为完整性。本框架述及信息恢复、传送和管理中的数据完整性。

本框架:

a) 定义完整性的基本概念；

b) 确定可能的完整性机制类；

c) 定义每一类完整性机制的设施；

d) 确定为支持完整性机制的管理需求；

e) 述及完整性机制和其支撑的服务与其他安全服务和机制的相互关系。

本框架中描述的某些规程通过密码技术的应用实现完整性。使用本框架不依赖于特定密码或其他算法的使用，尽管某种完整性机制类可能依赖于特定的算法性质。

本框架述及的完整性是指数据值的不变性，而不是数据被认为所代表的信息的不变性。其他形式的不变性亦排除在外。

6.7 第7部分：安全审计和告警

本框架：

a) 定义安全审计和告警的基本概念；

b) 提供安全审计和告警的通用模型；

c) 确定安全审计和告警服务与其他安全服务的关系。

正如其他安全服务一样，安全审计只能在已定义安全政策的上下文中提供。安全政策将由安全域中的安全机构定义。基于本框架的标准所说明的机制应该能够支持各种的安全政策。

6.8 密钥管理

密钥管理框架(GB/T 17901.1)与其他安全框架间的特殊关系在于其涉及到那些并非直接与GB/T9387.2中确定的安全服务有关的功能。那些功能适用于加密或数字签名适用的任何信息技术环境。

本框架：

a) 确定密钥管理的目的；

b) 描述密钥管理机制基于的通用模型；

c) 定义对于这个多部分标准各部分公用的密钥管理的基本概念；

d) 定义密钥管理服务；

e) 确定密钥管理机制的特征；

f) 规定密钥在其生存期内的管理需求；

g) 描述密钥在其生存期内的管理框架。

7 公共概念

许多概念被用于多个安全框架中。本标准定义这些概念以用于本系列标准其余的部分中。

7.1 安全信息

安全信息(SI)是实现安全服务所需要的信息。安全信息包括：

——安全政策规则；

——实现具体安全服务的信息，如鉴别信息(AI)和访问控制信息(ACI)；

——与安全机制相关的信息，如安全标签、密码校验值、安全证书和安全权标。

多个安全框架公共SI的类型在第8章中讨论。

7.2 安全域

安全域是由单个安全机构为特定的与安全相关的活动制定的安全政策下的元素集合。安全域的活动包括来自于该安全域的、或可能来自于其他安全域的一个或多个元素。

活动包括：

——对元素的访问；

——OSI(N)层连接的建立或使用；

——与具体管理功能相关的操作；

——包含公证的抗抵赖操作。

活动可以是安全相关的，即使它现在不是能够强制实施有关其使用的任意政策的机制的主体。特别是，不能防止发生在任意元素组的活动能够是与安全相关的，并且将来可以变成为控制机制的主体。

开放系统环境中安全域元素的例子包括逻辑元素和物理元素，如实开放系统、应用进程、(N)实体、(N)协议数据单元、中继以及人类用户的实开放系统等。存在安全域中的人类用户必须与其他元素区分开的某些情形。在这类情况下，为区分非人类元素，将使用术语“数据客体”。

7.2.1 安全政策和安全政策规则

安全政策以通用术语表达了安全域的安全需求。例如，安全政策可以确定应用于在具体环境下操作的安全域中所有成员的需求，或应用于安全域中所有信息的需求。安全政策的实现将导致满足这些安全政策的安全服务被确定，并且将会选择若干安全机制以便实现这些安全服务。选择哪些安全机制的决策受到所预见的威胁和所保护的资源价值的影响。

安全政策一般被描述成类似自然语言中的普遍原则。这些原则反映了特定组织或安全域成员的安全需求。在这些安全需求被反映在实开放系统之前，安全政策必须被细化以便能够从中推导出一组安全政策。作为安全政策规则解释这些需求是一项工程活动。安全政策通过允许使用某种行动或禁止特定行为来限制违背该安全政策的元素的行为。安全政策还可以给予元素参与特定活动的许可。这是一个较包含在GB/T 9387.2中的安全政策更广义的安全政策解释，GB/T 9387.2中的安全政策只与OSI有关。特定安全服务相关的安全政策将在那些服务的安全框架中讨论。

安全域的安全政策规则包括两种类型，即在安全域之内活动的安全政策规则和安全域之间活动的安全政策规则。后种类型的安全政策规则被称之为安全的交互规则。安全政策还可以定义哪些规则应用于与其他所有安全域的关系，哪些规则应用于与特定安全域的关系。

安全域的安全政策规则必须在系统变化或这些活动和安全域的安全政策被修改时仍保持有效。

注：安全框架不涉及安全政策的下列方面：

——建立或维护安全政策一方本身；

——建立或维护安全政策的过程；

——安全政策的内容；

——绑定安全政策到安全域的规程。

7.2.2 安全域机构

安全域机构是负责实现安全域的安全政策的安全机构。

安全域机构：

——可以是一个复合实体；这种实体必须是可标识的；

——取决于安全域可能遵守的任何安全政策，可以委派实现这个安全政策的责任给一个或多个实体；

——具有对安全域中元素的权威。

注：如果安全域权威已经决定不强加任何约束，安全政策可以为空。

如果两个安全域机构是被约束而协调其安全政策，则他们被称为是相互链接。

7.2.3 安全域间相互关系

安全域概念之所以被认为重要在于两个原因。即：

——它可以被用来描述安全如何被管理和实施；

——它可用作为构造包含在不同安全机构的元素的与安全相关活动的模型的构件。

安全域可以以一种或多种方式相关。这里讨论一些可能的联系。安全域的关系必须被反映在由其安全机构商定的安全域的安全政策中。这些关系以这些安全域的元素和活动的方式被说明，并且被反映在每一个相关的安全域的安全交互规则中。某些特殊的安全域的关系在本条的剩余部分描述。许多其

他的安全域关系也是可能的。

a) 两个安全域被称为相互孤立的，如果他们没有公共的数据客体，没有公共的行为，即没有相互作用；

b) 两个安全域被称为相互独立的，如果：

——它们没有公共的数据客体；

——每一个安全域内的活动只由其自身的安全政策(和相应的安全政策规则组)所约束；

——这些安全域的安全机构未被限定协调其安全政策。

两个或多个独立的安全域可以选择达成一个协调其间信息共享的协定。

c) 安全域 A 被称为是另外一个安全域 B 的安全子域，当且仅当：

——A 的元素集合是 B 的元素集合的子集，或是与 B 的元素集合相同；

——A 中的活动集合是 B 中的活动集合的子集，或是与 B 的活动集合相同；

——A 的控制权限是由 B 的安全机构委派给 A 的安全机构的；

——A 的安全政策与 B 的安全政策无冲突。如果需要并且为 B 的安全政策所允许，A 可以引入新的安全政策。

注：子集可以等于全集。安全子域可以形成于某些活动类的安全超域元素全集的这种极端情况下，或形成于安全超域元素全集的某些子集的所有活动类的另一种极端情况下。在这两种极端情况之间可能存在很多变种。

d) 当且仅当 B 是 A 的安全子域时，安全域 A 被称为另一个安全域 B 的安全超域。

注：安全框架不要求任意特殊协议、规范或实现支持孤立、独立、子域或超域的概念。

7.2.4 安全交互规则的建立

为了能够在安全域间交换信息，必须存在一组商定的用于该交换的安全政策规则。这些安全政策规则被称为安全交互规则。它们是每个安全域的安全政策规则的一部分。安全交互规则能够使公共的安全服务和机制通过协商被选择，并且能够使每一个安全域的安全信息项通过映射相互相关。为支持安全交互规则所需安全管理信息可以在安全域间交换。依赖于安全域间的关系不同，安全交互规则可以由不同方式决定。

对于独立安全域间的安全交互，安全交互规则必须由安全域的安全机构商定。

对于安全子域间的安全交互，安全交互规则必须由安全超域的安全机构建立。如果为安全超域的安全政策所允许，安全子域可以建立自己的安全交互规则。

7.2.5 域间的安全信息传送

安全交互规则自身可以构成安全信息，并且这种安全信息可能需要在安全域间传送。应考虑下列情况：

——安全信息在每个安全域中的语义和代表意义相同，即不需要翻译。

——安全信息在每个安全域中的语义是等同的，但代表的意义不同。即安全信息的描述方式不同，语法翻译是必需的。

——安全信息在每个安全域中的语义和代表意义都不同，即安全交互规则必须规定一个安全域中的安全信息如何被翻译成另一个安全域中的安全信息。语法翻译可能也是需要的。

7.3 具体安全服务的安全政策的考虑

访问控制机制可以被用于某些保密性服务或完整性服务的实现中。在这种情况下，涉及保密性服务或完整性服务的实现的安全政策规则必须描述访问控制机制将如何被使用。访问控制机制以发起方和目标(定义于本系列标准的第 3 部分，即 ISO/IEC 10181-3)形式描述。安全政策规则定义了完整性和保密性政策中的实体、信息和数据项是如何与访问控制机制中的发起方和目的方相关的。

保密性政策以哪些实体可以检查信息项的形式定义。由发起方到目的方的动作信息被显现给第三方有两种途径：首先动作的结果可能给发起方提供一些目的方的信息；其次动作的请求可能给目的方提供发起方的信息。当访问控制机制被用于提供保密性服务时，试图获取信息的实体被认为是发起方，信

息项被认为是目的方。

完整性政策以哪些实体可以修改数据项的形式定义。有两种途径使发起方到目的方的动作可能会引起数据被修改:首先这个动作可能直接引起包含在目的方内的数据被修改;其次动作的结果可以引起包含在发起方内的数据被修改。当访问控制机制被用于提供完整服务时,试图修改数据的实体被认为是发起方,数据项被认为是目标。

7.4 可信实体

一个实体在安全政策的上下文中被称之为对于某些活动类是可信,如果这个实体或是通过执行了其被认为不会执行的动作,或是未成功执行其被认为会执行的动作而违犯了安全政策。安全政策定义哪些实体是可信的,并且对于每一个实体定义了对于其是可信的活动集合。对于特定集合被认为是可信的实体不必要对于一个安全域中的所有活动集合都是可信的。

安全政策中对于一个实体应该以特定方式行事的声明不绝对保证这个实体将会以那种方式表现该行为。因此,安全政策可能需要检测由可信实体误操作导致的安全政策违规的动作的手段。能够误操作而不被发现的可信实体被称作无条件的可信实体。可能违犯安全政策,但不可能不被检测到的可信实体被称为有条件的可信实体。

一个可信实体可以对于其一个活动子集是无条件可信的而对于其另外一个活动子集是有条件可信的。这种实体在某些方面能够不被发现地违犯安全政策,但在另外某些方面可被发现违犯安全政策。

安全域的安全政策可以说明为非这个安全域的某个元素对这个安全域内的某些活动集合是可信的。安全交互规则(正如 7.2.4 中所讨论)可以定义安全域中的实体如何与安全域之外的可信实体交互。

7.5 可信

实体 X 被称为对实体 Y(对于某个活动集合)可信的当且仅当在特定情况下对于某些行为 X 依赖于 Y。

可信未必是相互的。一个非可信的实体可以利用可信实体提供的服务。可信是相互情形的一个例子是:两个可信实体在合作执行一个活动时,并且两个中的每一个实体都依赖于对方以辅助其实施安全政策。

可信未必是可传递的。安全政策可以定义在具体实例中可信关系的传递性。如果实体 A 依赖于由可信的实体 B 提供的服务,实体 B 依赖于由可信的实体 C 提供的服务,则实体 A 可能在特定方式不直接地依赖于实体 C 行事。在某种情况下,可信是传递的。但在其他情形下,B 可以采取某种方式确保 C 的误操作不影响 A 的活动。在这种情况下,可信是不传递的。

7.6 可信第三方

可信第三方是一个就某些安全相关活动而言是可信的(在安全政策的上下文中)安全机构或其代理。

可信第三方的例子包括:

——鉴别中的可信第三方;

——抗抵赖中的公证或时间戳服务;

——密钥管理中的密钥分发中心。

8 通用安全信息

在多个安全框架中使用某些类型的安全信息要求。本章描述安全信息的这些类型。

在安全框架中所描述的安全机制通常包括需相互交换的安全信息,如在交互中需要安全服务的实体之间的安全信息,或在安全机构和交互的实体间的安全信息。这些框架描述的机制所使用的安全信息的四种公共格式如下:

——用于指示适用于某个元素、通信信道或数据项的安全标签;

——用于检测数据项变化的密码校验值;

——用于保护从安全机构或从由一个或多个交互方使用的 TTP 获取的安全信息的安全证书；

——用于保护在交互方之间传递的安全信息的安全权标。

注：安全信息能够用几种不同的安全机制保护。某些安全机制是基于密码算法的使用，而另一些则使用物理方式。

8.1 安全标签

安全标签是用以联编某个元素、通信信道或数据项的安全属性集合。安全标签还显式地或隐含地指示安全机构负责创建和联编这个标识和适用于这个标签使用的安全政策。安全标签能够被用来支持安全服务的组合。

使用安全标签的例子包括：

——支持基于标签的访问控制方案，包括以提供完整性和/或保密性的访问控制应用；

——指示能够对于这种数据和其处理需求寄予的信任程度；

——指示对于这种数据和其处理需求的敏感性；

——指示保护、处置和其他处理需求。

8.2 密码校验值

密码校验值是通过对数据单元执行密码变换中推导出的信息。封印、数字签名和数字指纹是密码校验值的三个例子。

封印是通过使用对称密码算法和通信实体间共享的秘密密钥而计算出来的一种密码校验值的形式。封印被用来检测数据传送期间的修改。

数字签名是防止接收者进行伪造密码校验值，它使用私有密钥和非对称密码算法计算。数字签名的有效性验证要求使用相同的密码算法和相应的公开密钥。

注 1：尽管存在其他可以防止接收者伪造密码校验值的手段，(如使用防篡改的密码模块)，但安全框架使用的术语数字签名是指使用非对称密码算法产生的密码校验值。

注 2：在一些非对称密码算法中，数字签名的计算要求使用一个以上的私有密钥。当使用这类算法时，每个私有密钥的拥有者可以被限定为不同的实体。这确保了实体间必须合作以生成数字签名。

数字指纹是数据项的足以代表其独特性的一种特征，试图找出拥有相同数字指纹的另一数据项在计算上是不可行的。某些形式的密码校验值(如：给数据提供单向函数的结果)能够用来提供数字指纹。数字指纹能够由除密码算法外的其他手段提供。例如，数据项的拷贝就是一种数字指纹。

注 3：单向函数不等价于数字指纹。某些单向函数不适合创建数字指纹；同样，某些数字指纹不是使用单向函数生成。

注 4：使用非对称算法的数字签名的计算需花费很长时间因为一般来说非对称算法是计算密集型的。数字签名从数据的数字指纹计算要比从数据本身计算简单。这能够使性能得到改善，因为计算一个短的数字指纹的数字签名比计算一个长报文的数字签名更快。

密码校验值未必防止单个数据单元被重发。重发保护可以通过在数据中包含一些能够用来检测重发的信息的方法，如序列号或时间戳，或通过运用密码编链来实现。为提供防重发保护，该信息必须由被保护数据单元的接收者来检查。

8.3 安全证书

8.3.1 安全证书介绍

安全证书是由安全机构或可信第三方颁发的安全相关数据以及用于提供数据的完整性和数据源鉴别服务的安全信息的集合。安全证书包含一个对时间期间的标示以说明数据是否合法。

安全证书被用于把安全信息从安全机构(或可信第三方)传送到需要该信息执行安全功能的实体。安全证书可能包含用于一个以上安全服务的安全信息。

如其他安全框架中所描述，安全证书可以包含用于如下用途的 SI：

——访问控制；

——鉴别；

——完整性；

——保密性；

——抗抵赖；

——审计；

——密钥管理。

8.3.2 安全证书验证和编链

安全证书的验证包括核实其完整性、验证所声称的安全证书颁发者的身份、检查这个颁发者是否被授权创建这个安全证书。这些操作可能需要更多的 SI。

如果安全证书的验证者没有为验证安全证书所需的 SI，则来自另一个安全机构的安全证书可以被用来提供必需的 SI。这个过程可以被重复以提供安全证书链。安全证书链载有提供从某个已知安全机构(即其 SI 已经被建立的安全机构)到要求签发 SI 的实体间安全路径的 SI。

安全证书链应该仅当其符合由所有相关安全政策强加的限制时才能使用。链的存在是不充分的。只有其使用是为链的验证者和创建链中证书的安全机构间的可信关系所允许并且还为这些安全机构间的可信关系所允许时，链才应该被使用。这些信赖关系由证书链的验证者的安全政策和安全机构的安全政策定义。特别是，某些安全机构被认为可以可信地为另一些安全机构颁发安全证书，而另一些安全机构只被认为可信地为其所管理的实体颁发安全证书。

8.3.3 安全证书的撤消

包含在安全证书中的 SI 可能不再有效。例如，如果私有密钥被泄露，则相应的公开密钥便不能再使用，因此包含该公开密钥的安全证书应被撤消。

能够用于撤消安全证书的机制包括撤消证书和撤消列表证书。撤消证书是表明特定证书已被撤消的安全证书。撤消列表证书是确定已撤消安全证书的列表。

8.3.4 安全证书的重用

某些安全证书打算被用来支持一次以上的通信实例，同时其他证书只打算被使用一次。打算被使用多次的证书的例子定义于 GB/T 16264.8 中的鉴别证书。打算只被使用一次的安全证书的例子是授权单个访问的访问控制证书。打算只被使用一次的证书可以包含防止重用的信息(如一个唯一性编号)。

8.3.5 安全证书结构

安全证书的通用格式具有以下三个组成部分：

——所有安全证书需要的信息；

——特定于一个或多个安全服务的安全信息；

——控制或限制安全信息使用的信息。

所有安全证书需要的信息分为两类：

a) 提供完整性和数据源鉴别的信息(如密码校验值和被用来验证的显示信息)。由于提供了数据源鉴别服务，所以也必须提供安全证书所声称的源的身份指示。

b) 从其能够确定(如显式的有效期)或者推导出(如创建时间和隐式的有效期)有效期的信息。这可以避免安全证书的无限的重用，尽管安全证书在其有效期内可以被多次重用。

用于控制或限制安全信息使用的信息分为三类：

a) 用于保护安全证书免受非授权使用的信息，例如：

——标识其 SI 被包含在安全证书中的某个特定实体或者某些实体的信息(如可区分的标识符)；

——标识其被允许利用包含在这个安全证书中的 SI 的实体的信息；

——控制证书可以被使用的次数的信息；

——标识在其下这个安全证书必须被使用的安全政策的信息；

——为防止安全证书被盗的保护方法和相关参数(请参见附录 A 中的例子)；

——用于防止重发(如唯一性编号或盘问口令)的信息。

b) 能够被用于辅助安全审计的信息，例如：

——就由同一安全机构或代理而言，所颁发的所有安全证书是唯一的安全证书引用标识符（如序列号）；

——最初为其颁发安全证书的实体的身份（用于审计目的）。

c）能够被用于辅助安全恢复的信息，例如：

——能够用于撤消具体安全证书的安全证书引用标识符；

——能够用于撤消一组安全证书的安全证书组标识符。

8.4 安全权标

安全权标是由一个或多个安全服务保护的数据以及用于提供这些安全服务的安全信息的集合，其在通信实体间传送。安全权标可以根据由谁创建和哪些安全服务被用于保护其内容而分类。

由安全机构颁发和由完整性和数据源鉴别服务保护的安全权标被称为安全证书（见 8.3）。

许多安全机制要求在两个通信实体间的安全信息的完整性—保护交换，其中通信实体都不是安全机构。用于实现这种完整性—保护的交换的安全权标不是安全证书，因为生成它们的实体不是安全机构。这类安全权标被称为完整性保护安全权标。

所有的完整性保护安全权标都包含下列信息：

——既提供完整性也提供数据源鉴别的信息（如密码校验值和用于验证它的信息的指示）。

一个完整性保护安全权标可以包含一个或多个如下的附加信息项：

——从其能够确定有效期的信息；

——用于重发保护的信息（如唯一性编号）。

9 通用安全设施

许多设施被要求用于多个安全框架中。本章定义在其他的安全框架中使用的这些设施。

9.1 与管理相关的设施

本条确定管理设施的通用类型。这些管理设施的子类可能存在，其可以特定于某些特定的安全机制。

9.1.1 安装 SI

这个设施建立一个绑定到某个元素的 SI 的初始集合。

9.1.2 卸载 SI

这个设施引起某个实体从安全域中被去除，通过撤消声明这个实体是这个安全域成员的 SI。

9.1.3 更改 SI

这个设施被引用以便修改与某个元素相关的 SI。

9.1.4 确证 SI

这个设施将 SI 集合绑定到某个元素。确证 SI 设施由安全机构或其代理引用。

9.1.5 非确证 SI

本设施使与某个元素相关的任何 SI 的使用都被失能。非确证 SI 设施由安全机构或其代理调用。为审计的目的和确保其一直是失能的，被非确证 SI 设施失能的 SI 可以一直保留在系统中。

9.1.6 失能/重使能安全服务

本设施失能/重使能安全服务的已确定方面。

9.1.7 注册

本设施使安全机构记录某些与某个实体相关的安全信息。注册设施可以由非安全机构的某个实体调用。例如，如果一个希望加入到安全域中的实体能够使用注册设施去通知安全机构其希望加入到这个安全域中。

9.1.8 取消注册

本设施使某个元素被从安全域中删除且与其相关的 SI 被撤消。此设施由安全机构或其代理使用。