ICS 35.100.70
L 79

中华人民共和国国家标准

GB/T 16264.8—2005/ISO/IEC 9594-8:2001
代替 GB/T 16264.8—1996

信息技术　开放系统互连　目录
第8部分:公钥和属性证书框架

Information technology—Open Systems Interconnection—The Directory—Part 8:Public-key and attribute certificate frameworks

(ISO/IEC 9594-8:2001,IDT)

2005-05-25 发布　　2005-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 16264《信息技术　开放系统互连　目录》分为十个部分：

第1部分：概念、模型和服务的概述

第2部分：模型

第3部分：抽象服务定义

第4部分：分布式操作规程

第5部分：协议规范

第6部分：选择属性类型

第7部分：选择客体类

第8部分：公钥和属性证书框架

第9部分：重复(尚未制定)

第10部分：用于目录行政管理的系统管理用法(尚未制定)

本部分为GB/T 16264的第8部分，等同采用ISO/IEC 9594-8:2001《信息技术　开放系统互连　目录　第8部分：公钥和属性证书框架》。

本部分代替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》。本部分与GB/T 16264.8—1996相比，主要变化如下：

——本部分描述了一套作为所有安全服务基础的框架，并规定了在鉴别及其他服务方面的安全要求。本部分还特别规定了以下三种框架：

- 公钥证书框架；
- 属性证书框架；
- 鉴别服务框架。

——定义各种应用使用该鉴别信息执行鉴别的三种方法，并描述如何通过鉴别来支持其他安全服务。

本部分的附录A、附录C、附录D、附录E、附录G和附录H为资料性附录，附录B和附录F为规范性附录。

本部分由中华人民共和国信息产业部提出。

本部分由全国信息安全标准化技术委员会归口。

本部分主要起草单位：中国电子技术标准化研究所。

本部分主要起草人：吴志刚、赵菁华、王颜尊、黄家英、郑洪仁、李丹、高能。

引　言

GB/T 16264 的本部分连同其他几部分一起，用于提供目录服务的信息处理系统的互连。所有这样的系统连同它们所拥有的目录信息，可以看作一个整体，称为“目录”。目录中收录的信息在总体上称为目录信息库(DIB)，它可用于简化诸如 OSI 应用实体、人、终端，以及分布列表等客体之间的通信。

目录在开放系统互连中起着极其重要的作用，其目的是允许在互连标准之下使用最少的技术协定，完成下列各类信息处理系统的互连：

- 来自不同厂家的信息处理系统；
- 处在不同机构的信息处理系统；
- 具有不同复杂程度的信息处理系统；
- 不同年代的信息处理系统。

许多应用都有保护信息的通信免受威胁的安全要求。实际上，所有的安全服务都依赖于通信各方的身份被可靠地认知，即，鉴别。

本部分定义了一个公钥证书框架。这个框架包括了用于描述证书本身和撤销发布证书不再被信任的通知的数据对象规范。本部分中定义的公钥证书框架虽然定义了一些公钥基础设施(PKI)的关键组件，但却不是 PKI 的全部组件。本部分提供了用于建立所有的 PKI 及其规范的基础。

同样的，本部分定义了属性证书的框架。这个框架包括了用于描述证书本身和撤销发布证书不再被信任的通知的数据对象规范。本部分中定义的属性证书框架虽然定义了一些特权管理基础设施(PMI)的关键组件，但却不是 PMI 的全部组件。本部分提供了用于建立所有的 PMI 及其规范的基础。

本部分还定义了目录中的 PKI 和 PMI 对象的持有者信息及存储值和现有值之间的比较。

本部分定义了用于目录向其用户提供鉴别服务的框架。

本部分提供了能被其他标准制定组织和行业论坛定义的行业的基础框架。在这些框架中，许多特性定义为可选的，可以在特定环境中通过描述委托使用。此版为标准的第四版，是在第三版基础上的技术性的修订和增强，但它并不替代第三版。目前实现时仍可使用第三版。然而，在某些方面本部分不支持第三版(即，所报告的缺陷不再予以解决)。推荐尽快执行第四版。

本部分凡涉及密码算法相关内容，按国家有关法规实施。

本部分中所引用的 MD5、SHA-1、RSA、DES、DH 和 DSA 密码算法为举例性说明，具体使用时均须采用国家商用密码管理委员会批准的相应算法。

信息技术　开放系统互连　目录
第8部分:公钥和属性证书框架

第一篇　综　　述

1　范围

本部分描述了一套作为所有安全服务基础的框架,并规定了在鉴别及其他服务方面的安全要求。本部分特别规定了以下三种框架:

- 公钥证书框架;
- 属性证书框架;
- 鉴别服务框架。

本部分中的公钥证书框架包含了公钥基础设施(PKI)信息对象(如公钥证书和证书撤销列表(CRL)等)的定义。属性证书框架包含了特权管理基础设施(PMI)信息对象(如属性证书和属性撤销列表(ACRL)等)的定义。该部分还提供了用于发布证书、管理证书、使用证书以及撤销证书的框架。在规定的证书类型格式和撤销列表模式格式中都包括了扩展机制。本部分同时还分别包括这两种格式一套标准的扩展项,这些扩展项在PKI和PMI的应用中是普遍实用的。本部分包括了模式构件(如对象类、属性类型和用于在目录中存储PKI对象和PMI对象的匹配规则)。超出这些框架的其他PKI和PMI要素(如密钥和证书管理协议、操作协议、附加证书和CRL扩展)将由其他标准机构(如ISO TC68,IETF等)制定。

本部分定义的鉴别模式具有普遍性,并可应用于不同类型的应用程序和环境中。

对目录使用公钥证书和属性证书,本部分还规定了目录使用这两种证书的使用框架。目录使用公钥技术(如证书)实现强鉴别,签名操作和/或加密操作,以及签名数据和/或加密的数据在目录中存储。目录利用属性证书能够实现基于规则的访问控制。本部分只规定框架方面的内容,但有关目录使用这些框架的完整规定、目录所提供的相关服务及其构件在目录系列标准中进行规定。

本部分还涉及鉴别服务框架方面的如下内容:

- 具体说明了目录拥有的鉴别信息的格式;
- 描述如何从目录中获得鉴别信息;
- 说明如何在目录中构成和存放鉴别信息的假设;
- 定义各种应用使用该鉴别信息执行鉴别的三种方法,并描述如何通过鉴别来支持其他安全服务。

本部分描述了两级鉴别:使用口令作为自称身份验证的弱鉴别;包括使用密码技术形成凭证的强鉴别。弱鉴别只提供一些有限的保护,以避免非授权的访问,只有强鉴别才可用作提供安全服务的基础。本部分不准备为鉴别建立一个通用框架,但对于那些技术已经成熟的应用来说本部分可能是通用的,因为这些技术对它们已经足够了。

在一个已定义的安全策略上下文中仅能提供鉴别(和其他安全服务)。因标准提供的服务而受限制的用户安全策略,由一个应用的用户自己来定义。

由使用本鉴别框架定义的应用标准来指定必须执行的协议交换,以便根据从目录中获取的鉴别信息来完成鉴别。应用从目录中获取凭证的协议称作目录访问协议(DAP),由ITU-T X.519|ISO/IEC 9594-5规定。