ICS 35.100
L 79

中华人民共和国国家标准

GB/T 16264.8—1996
idt ISO/IEC 9594-8:1990

信息技术 开放系统互连 目录 第8部分:鉴别框架

Information technology—Open systems interconnection—The directory Part 8:Authentication framework

1996-03-22发布 1996-10-01实施

国家技术监督局 发布

中 华 人 民 共 和 国
国 家 标 准
信息技术 开放系统互连 目录
第8部分：鉴别框架
GB/T 16264.8—1996
*
中国标准出版社出版发行
北京西城区复兴门外三里河北街16号
邮政编码：100045
http://www.bzcbs.com
电话：63787337、63787447
1997年3月第一版 2005年1月电子版制作
*
书号：155066·1-13557

目　　次

前　言

本标准等同采用国际标准 ISO/IEC 9594-8:1990《信息技术　开放系统互连目录　第 8 部分:鉴别框架》和 ISO/IEC 9594-8:1990/Cor.1:1991《信息技术　开发系统互连　目录　第 8 部分:鉴别框架技术修改 1》。

根据 ISO/IEC 9594-8:1990/Cor.1:1991,本标准对 7.2、7.6、9.4 和 C5.2 作了修改,并删去了 D2 章。

通过制定这项国家标准,以便为信息处理的目录服务提供统一的鉴别框架。

GB/T 16264 在《信息技术　开放系统互连　目录》总标题下,目前包括以下 8 个部分:

第 1 部分(即 GB/T 16264.1):概念、模型和服务的概述;

第 2 部分(即 GB/T 16264.2):模型;

第 3 部分(即 GB/T 16264.3):抽象服务定义;

第 4 部分(即 GB/T 16264.4):分布操作过程;

第 5 部分(即 GB/T 16264.5):协议规范;

第 6 部分(即 GB/T 16264.6):选择属性类型;

第 7 部分(即 GB/T 16264.7):选择客体类;

第 8 部分(即 GB/T 16264.8):鉴别框架。

本标准的附录 G 是标准的附录;

本标准的附录 A、B、C、D、E、F 和 H 是提示的附录。

本标准由中华人民共和国电子工业部提出。

本标准由电子工业部标准化研究所归口。

本标准起草单位:电子工业部标准化研究所、华北计算技术研究所。

本标准主要起草人:郑洪仁、李卫国、黄家英、冯惠。

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 9594.8 是由 ISO/IEC JTC1"信息技术"联合技术委员会制定的。

ISO/IEC 9594 在《信息技术　开放系统互连　目录》总标题下,目前包括以下 8 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:鉴别框架

附录 G 构成为 ISO/IEC 9594.8 的一部分,而附录 A、B、C、D、E、F 和 H 仅提供参考信息。

引　言

0.1　本标准，连同本系列标准的其他几部分一起，便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。

0.2　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外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。

0.3　许多应用都有保护信息的通信免受威胁的安全要求。附录A概要描述了一些常见的威胁以及可用于保护信息免受这些威胁的安全服务和安全机制。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。

0.4　本标准借助目录给其用户的鉴别服务定义了一个框架。这些用户不仅包括其他应用和服务，还包括目录本身。目录常用来满足鉴别和其他安全服务的需要，因为目录是通信各方获得作为相互鉴别的基础的鉴别信息的一个自然场所；同时，在目录中还保存了用于满足通信请求并且在通信发生之前必须获得的其他信息。用这种方法还可以从目录中获得一个潜在通信伙伴的鉴别信息，类似于获得一个地址。由于以通信为目的的目录的适用范围很广泛，可以预期，许多应用都将广泛地使用这个鉴别框架。

中华人民共和国国家标准

信息技术　开放系统互连　目录 第8部分：鉴别框架

GB/T 16264.8—1996
idt ISO/IEC 9594-8:1990

Information technology—Open systems interconnection—The directory Part 8:Authentication framework

第一篇　综　述

1　范围

1.1　本标准：

- 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，并描述鉴别如何支持其他安全服务。

1.2　本标准描述了两级鉴别：简单鉴别，使用口令作为自称身份的一个验证；强鉴别，包括使用密码技术形成凭证。简单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。本标准不准备为鉴别建立一个通用框架，但本标准对于认为那些技术已经足够的应用来说可能是通用的，因为这些技术对它们已经足够了。

1.3　在一个已定义的安全策略上下文中仅提供鉴别（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。

1.4　由使用本鉴别框架定义的应用的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 GB/T 16264.5 规定。

1.5　本标准中规定的强鉴别方法以公开密钥密码体制为基础。这种体制的主要优点是可以将用户证书作为目录的属性保存在目录中，并允许在目录系统中自由交换，目录的用户也可以采用与获取其他目录信息同样的方法获取用户证书。用户证书可以采用‘脱机’方式形成，并由其创建者置入目录中。用户证书的生成应由完全独立于目录中的任何 DSA 的‘证明职能机构’负责。尤其是，不应对目录提供者存储或交换用户证书所采用的安全方法作特殊的要求。

附录 B 给出了公开密钥密码的概要介绍。

1.6　在通常情况下，鉴别框架应独立于所采用的具有 6.1 所描述的特性的某种加密算法，也就是说，可以采用多种不同的加密算法。然而，想要相互鉴别的两个用户则支持采用相同的加密算法，从而确保进行正确的鉴别。因此，在一组相关的应用的上下文中，选择一种单一的算法将会增强用户进行安全鉴别和通信的一致性。

附录 C 给出了公开密钥加密算法的一个示例。

1.7　同样，想要相互鉴别的两个用户必须支持相同的散列函数（见 3.3.6），散列函数主要用于生成凭证和鉴别权标。同样，从原理上说，也可以采用多种散列函数，但这要以减小用户鉴别的一致性为代价。

附录 D 给出了散列函数的概要介绍及示例。

国家技术监督局 1996-03-22 批准　　1996-10-01 实施