<<信息安全标准汇编>>

图书基本信息

书名：<<信息安全标准汇编>>

13位ISBN编号：9787506651103

10位ISBN编号：7506651106

出版时间：2009-1

出版时间：中国标准出版社第四编辑室 中国标准出版社 (2009-01出版)

作者：中国标准出版社第四编辑室 编

前言

GB／T17903在总标题《信息技术安全技术抗抵赖》下，由以下几部分组成：——第1部分：概述；——第2部分：采用对称技术的机制；——第3部分：采用非对称技术的机制。
本部分是GB／T17903的第1部分，等同采用ISO／IEC13888-1：2004《信息技术安全技术抗抵赖第1部分：概述》，仅有编辑性修改。
本部分代替GB／T17903．1-1999《信息技术安全技术抗抵赖第1部分：概述》。
本部分与GB17903．1-1999相比，主要差别如下：——本部分修订了第3章中的部分术语和定义。
——本部分对部分叙述进行了文字修订，并把第11章中的“ NRDT ”修正为“ NROT ”。
——本部分对第5章和第6章的顺序进行了调整。
——本部分删除了原附录A。
本部分由全国信息安全标准化技术委员会提出并归口。
本部分主要起草单位：中国科学院软件研究所信息安全国家重点实验室。
本部分主要起草人：张振峰、冯登国。
本部分所代替标准的历次版本发布情况为：——GB／T17903．1-1999。

内容概要

《信息安全标准汇编:技术与机制卷授权与访问控制分册》由以下几部分组成：——第1部分：概述；——第2部分：采用对称技术的机制；——第3部分：采用非对称技术的机制。
本部分是GB／T17903的第1部分，等同采用ISO／IEC13888-1：2004《信息技术安全技术抗抵赖第1部分：概述》，仅有编辑性修改。

本部分代替GB／T17903.1-1999《信息技术安全技术抗抵赖第1部分：概述》。
本部分与GB17903.1-1999相比，主要差别如下：
——本部分修订了第3章中的部分术语和定义。

——本部分对部分叙述进行了文字修订，并把第11章中的“ NRDT ”修正为“ NROT ”。

——本部分对第5章和第6章的顺序进行了调整。

——本部分删除了原附录A。

本部分由全国信息安全标准化技术委员会提出并归口。

本部分主要起草单位：中国科学院软件研究所信息安全国家重点实验室。

本部分主要起草人：张振峰、冯登国。

本部分所代替标准的历次版本发布情况为：——GB／T17903.1-1999。

<<信息安全标准汇编>>

书籍目录

章节摘录

插图：6.2.3 证书扩展6.2.3.1 证书扩展概述在GB／T16264.8-2005中定义了一套标准扩展集合。
扩展由三部分组成：扩展名称、关键性标识位和扩展取值。
在GB／T16264.8-2005中做了如下规定：客户如果不能处理设置了关键性标识位的扩展，就不能验证证书是否有效。
标准化的扩展可以分为四类：密钥和策略信息；主体和颁发者的特征；验证路径限制；CRL标识扩展。
6.2.3.2 密钥和策略信息此类扩展用于区分特定的公钥和证书，它们可以用于区别具有多个证书的证书认证机构（CA）中某一特定的公钥／证书，有助于客户查找某个特定的CA证书，以便建立验证路径。
这些扩展可以限制密钥用途，提供CA证书中关于策略映射的信息。
a）权威密钥标识符扩展authorituKeyIdentifiel提供了一种区别签名证书的特定私钥的手段，标识性信息既可以基于密钥标识符，也可以基于颁布者名字和序列号。
在本标准中，使用密钥标识符的方法。
本扩展用于具有多个签名密钥的颁发者（既可能是多个密钥对，也可能是正在进行密钥更换），证书认证机构（CA）应当能够产生本扩展，而且客户应能查找和验证具有多个数字签名密钥的证书颁发者CA的验证路径。
建议客户既能够处理密钥标识符，又能够处理由证书颁发者和证书序列号组成的密钥标识符，便于找到验证路径。
b）主体密钥标识符本字段用于区别一个主体所拥有的多个密钥，在每个已颁发的证书中都应当包含本字段，本扩展应当是非关键的。

编辑推荐

《信息安全标准汇编:技术与机制卷授权与访问控制分册》是由中国标准出版社出版的。

<<信息安全标准汇编>>

版权说明