



中华人民共和国国家标准

GB/T 17901.1—2020
代替 GB/T 17901.1—1999

信息技术 安全技术 密钥管理 第 1 部分：框架

Information technology—Security techniques—Key management—
Part 1: Framework

(ISO/IEC 11770-1:2010, MOD)

2020-03-06 发布

2020-10-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言	Ⅲ
引言	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号和缩略语	3
4.1 符号	3
4.2 缩略语	3
5 密钥管理的一般模型	4
5.1 概述	4
5.2 密钥保护	4
5.3 密钥生存周期的一般模型	5
6 密钥管理的基本内容	6
6.1 密钥管理服务	6
6.2 支持服务	9
7 两实体间密钥分发的概念模型	10
7.1 密钥分发概述	10
7.2 通信实体间的密钥分发	10
7.3 单域密钥分发	10
7.4 域间的密钥分发	12
8 特定服务的提供者	13
附录 A (资料性附录) 密钥管理面临的安全威胁	14
附录 B (资料性附录) 密码应用分类	15
附录 C (资料性附录) 密钥管理信息对象	17
参考文献	18