ICS 35.040
L 80

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
国家标准化管理委员会　发布

目　　次

前　言

GB/T 17901《信息技术　安全技术　密钥管理》拟分为6个部分：

——第1部分：框架；

——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；

——第4部分：基于弱秘密的机制；

——第5部分：群组密钥管理；

——第6部分：密钥派生。

本部分为GB/T 17901的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 17901.1—1999《信息技术　安全技术　密钥管理　第1部分：框架》，与GB/T 17901.1—1999相比，主要技术变化如下：

——在规范性引用文件中增加了新的引用文件(见第2章)；

——删除了“解密、加密、密钥确认、密钥控制、密钥分发中心(KDC)、密钥材料、密钥管理、密钥转换中心(KTC)、公开密钥信息、随机数、顺序号”的术语和定义，增加了“杂凑函数、密钥派生函数、密钥建立、密钥权标、消息鉴别码、签名系统”的术语和定义(见第3章，1999年版的第3章)；

——增加了第4章“符号和缩略语”(见第4章)；

——将1999年版的第4章“密钥管理综述”修改为第5章“密钥管理的一般模型”，删除了1999年版的4.1.2，增加了5.1、5.3.1，并对部分内容进行了修改(见第5章，1999年版的第4章)；

——将1999年版的第6章“密钥分发概念模型”修改为第7章“两实体间密钥分发的概念模型”，增加了7.1，并对部分内容进行了修改(见第7章，1999年版的第6章)；

——删除了1999年版的附录D，相关内容与现有国家标准和密码行业标准保持一致。

本部分使用重新起草法修改采用ISO/IEC 11770-1:2010《信息技术　安全技术　密钥管理　第1部分：框架》。

本部分与ISO/IEC 11770-1:2010相比在结构上有调整，增加了第2章，后续条款号依次改变，调整4.2.3～4.2.5为5.2.2、5.2.3.1和5.2.3.2，调整附录B为附录C，附录C为附录B。

本部分与ISO/IEC 11770-1:2010的技术性差异及其原因如下：

——增加了第2章规范性引用文件(见第2章)；

——删除了部分术语和定义(见ISO/IEC 11770-1:2010的第2章)；

——删除了“CA”和“RA”的符号(见ISO/IEC 11770-1:2010的3.1)；

——在第5章明确了“应采用国家密码管理部门认可的密码算法”，并将ISO/IEC 11770-1:2010所引用的密码算法标准修改为引用我国对应的密码算法标准，以便于使用(见第5章)。

本部分还做了下列编辑性修改：

——删除ISO/IEC 11770-1:2010的资料性附录D，相关内容与现有国家标准和密码行业标准保持一致。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程实验室、

中关村无线网络安全产业联盟、国家密码管理局商用密码检测中心、北京大学深圳研究生院、中国电子科技集团公司第三十研究所、国家无线电监测中心检测中心、中国电子技术标准化研究院、中国通用技术研究院、中国网络安全审查技术与认证中心、天津市无线电监测站、北京计算机技术及应用研究所、天津市电子机电产品检测中心、重庆邮电大学。

本部分主要起草人：杜志强、李琴、郎元、朱跃生、刘科伟、周国良、陶洪波、王月辉、铁满霞、张变玲、彭潇、李冰、许玉娜、黄振海、布宁、张璐璐、于光明、颜湘、张国强、刘景莉、李冬、商钧、赵慧、王莹、朱正美、高德龙、郑骊、熊克琦、黄奎刚、龙昭华、吴冬宇。

本部分所代替标准的历次版本发布情况为：

——GB/T 17901.1—1999。

引　言

在信息技术中，采用密码机制保护数据不被非法窃取或篡改、实现实体鉴别和抗抵赖的需求与日俱增。这些机制的安全性和可靠性直接取决于对密钥的管理和保护。如果密钥管理有薄弱环节，那么将使其声称的密码功能都失效，因此安全管理密钥对于将密码功能集成到系统中至关重要。密钥管理的目的是提供用于对称或非对称密码机制中的密钥处理程序。

本部分修改采用 ISO/IEC 11770-1:2010《信息技术　安全技术　密钥管理　第1部分：框架》，适用于对通信密钥的管理。ISO/IEC 11770 定义了密钥管理的一般模型，它不依赖使用的特定密码算法。但是某些密钥分发机制取决于特定算法的特性，例如非对称算法特性。

如果密钥管理中需要使用抗抵赖功能，参见 GB/T 17903。

本部分描述了自动和人工两种密钥管理方法，包括数据元素框架以及用于获取密钥管理服务的操作流程，但对协议交换所需的细节不作详细说明。

同其他安全服务一样，密钥管理只在所定义的安全策略中提供密钥管理服务，但安全策略的定义超出本部分的范围。

密钥管理的根本问题是要参与各方确认密钥材料，向直接和间接用户保证其来源、完整性、即时性以及(秘密密钥情形下)保密性。密钥管理包括根据某一安全策略生成、存储、分发、删除和归档密钥(GB/T 9387.2—1995)等功能。

信息技术　安全技术　密钥管理
第1部分:框架

1　范围

GB/T 17901的本部分包含以下内容:

a)　建立密钥管理机制的通用模型;

b)　定义对GB/T 17901通用的密钥管理的基本概念;

c)　定义密钥管理服务的特征;

d)　规定对密钥在其生存周期内进行管理的通用原则;

e)　建立通信密钥分发的概念模型。

本部分适用于建立密钥管理模型和设计密钥管理方法。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 15843(所有部分)　信息技术　安全技术　实体鉴别[ISO/IEC 9798(所有部分)]

GB/T 17903.2　信息技术　安全技术　抗抵赖　第2部分:采用对称技术的机制(GB/T 17903.2—2008,ISO/IEC 13888-2:1998,IDT)

GB/T 18794.1　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)

GB/T 32907　信息安全技术　SM4分组密码算法

GB/T 32918(所有部分)　信息安全技术　SM2椭圆曲线公钥密码算法

GB/T 37092—2018　信息安全技术　密码模块安全要求

ISO/IEC 18014(所有部分)　信息技术　安全技术　时间戳服务(Information technology—Security techniques—Time-stamping services)

ISO/IEC 18031　信息技术　安全技术　随机数生成(Information technology—Security techniques—Random bit generation)

3　术语和定义

下列术语和定义适用于本文件。

3.1

非对称密码技术　asymmetric cryptographic technique

采用两种相关的变换,由公钥定义的公开变换和由私钥定义的私有变换的密码技术。

注:这两个变换具有如下特性,即对给定的公钥导出私钥在计算上是不可行的。

3.2

非对称密钥对　asymmetric key pair

一对相关的密钥,其中私有密钥规定私有变换,公开密钥规定公开变换。

[ISO/IEC 11770-3:2008,定义3.3]