ICS 35.040
L 80

中华人民共和国国家标准

GB/T 17901.3—2021

信息技术　安全技术　密钥管理
第3部分:采用非对称技术的机制

Information technology—Security techniques—Key management—Part 3:Mechanisms using asymmetric techniques

(ISO/IEC 11770-3:2015, MOD)

2021-03-09 发布　　2021-10-01 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3部分。

本部分按照GB/T 1.1—2009给出的的规则起草。

本部分使用重新起草法修改采用ISO/IEC 11770-3:2015《信息技术　安全技术　密钥管理　第3部分：采用非对称技术的机制》。

本部分与ISO/IEC 11770-3:2015的技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 删除了对ISO/IEC 10118、ISO/IEC 11770-1以及ISO/IEC 15946-1的引用；
- 增加了对GB/T 15843.3—2016、GB/T 17901.1—2020、GB/T 25069、GB/T 32905以及GB/T 32918系列标准的引用(见第2章)。

——删除了ISO/IEC 11770-3:2015中3.1～3.18和3.20～3.43的术语和定义，增加了3.1、3.2和3.4的术语和定义(见第3章)。

——增加了“本部分涉及使用椭圆曲线签名验证、公钥加解密的算法见GB/T 32918.2和GB/T 32918.4。”(见第5章)。

——修改了对附录C、附录D、附录E和附录F的引用关系(见第11章、第12章和第13章)。

——修改或删除了ISO/IEC 11770-3:2015中的附录C、附录D和附录E中与密钥管理具体实例相关的内容，并在附录C中增加对GB/T 32918.3—2016中规范的密钥派生函数的引用，在附录E中增加对GB/T 32918.3—2016规范的SM2密钥协商机制的引用。

——删除了ISO/IEC 11770-3:2015中的附录F和附录G。

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、北京大学深圳研究生院、国家密码管理局商用密码检测中心、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、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、王月辉、朱跃生、周国良、陶洪波、李琴、铁满霞、张变玲、井经涛、李志勇、李冰、彭潇、刘科伟、黄振海、许玉娜、于光明、郎元、郑骊、颜湘、张国强、刘景莉、李冬、朱正美、商钧、王莹、赵慧、高德龙、方华、熊克琦、李玉娇、龙昭华、吴冬宇。

信息技术　安全技术　密钥管理
第3部分:采用非对称技术的机制

1　范围

GB/T 17901的本部分定义了基于非对称密码技术的密钥管理机制的要求、密钥派生函数、余子式乘法、密钥承诺、密钥确认、密钥管理框架、密钥协商、密钥传递、公钥传递。

本部分拟达到如下目的:

a)　通过密钥协商建立一个共享密钥,用于实体A和实体B间的对称加密。在密钥协商机制中,密钥通过实体A和实体B交换的数据计算得到,任何实体一方不能预先确定共享密钥值。

b)　通过密钥传递建立一个共享密钥,用于实体A和实体B间的对称加密。在密钥传递机制中,密钥由实体A选择,采用非对称密码保护技术,传给实体B。

c)　通过密钥传递将实体A的公钥传给其他实体。在公钥传递机制中,实体A的公钥经鉴别后传给其他实体,但不需保密。

本部分定义的一些机制基于GB/T 15843.3—2016相对应的鉴别机制。

本部分不包含以下密钥管理内容:

a)　密钥生存期管理;

b)　产生或确定非对称密钥对的机制;

c)　密钥的存储、存档、删除等机制。

本部分适用于采用非对称技术实现密钥管理的系统的研制,也可指导该类系统的检测。

注:本部分定义的机制不涉及实体私钥的分发,由公钥签名系统对密钥交换消息进行签名进行操作。

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 15843.3—2016　信息技术　安全技术　实体鉴别　第3部分:采用数字签名技术的机制

GB/T 17901.1—2020　信息技术　安全技术　密钥管理　第1部分:框架

GB/T 25069　信息安全技术　术语

GB/T 32905　信息安全技术　SM3密码杂凑算法

GB/T 32918.1　信息安全技术　SM2椭圆曲线公钥密码算法　第1部分:总则

GB/T 32918.2　信息安全技术　SM2椭圆曲线公钥密码算法　第2部分:数字签名算法

GB/T 32918.3—2016　信息安全技术　SM2椭圆曲线公钥密码算法　第3部分:密钥交换协议

GB/T 32918.4　信息安全技术　SM2椭圆曲线公钥密码算法　第4部分:公钥加密算法

3　术语和定义

GB/T 17901.1—2020和GB/T 25069界定的以及下列术语和定义适用于本文件。