ICS 35.040
CCS L 80

中华人民共和国密码行业标准

GM/T 0091—2020

基于口令的密钥派生规范

Password-based key derivation specification

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本标准的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京信安世纪科技股份有限公司、格尔软件股份有限公司、北京数字认证股份有限公司、长春吉大正元信息技术股份有限公司、兴唐通信科技有限公司、卫士通信息产业股份有限公司、国家信息安全工程技术研究中心、山东得安信息技术有限公司、北京创原天地科技有限公司。

本文件主要起草人：汪宗斌、刘婷、郑强、傅大鹏、赵丽丽、王妮娜、赵闪、罗俊、张旭、周淑静、张庆勇、焦靖伟、史晓峰、马洪富。

基于口令的密钥派生规范

1 范围

本文件规定了基于口令的密钥派生规范，包括基于口令的密钥派生函数、基于口令的加密方案、基于口令的消息鉴别码。

本文件适用于证书与密钥迁移时利用口令来保护被迁移的密钥。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 15852.2 信息技术 安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制

GB/T 25069—2010 信息安全技术 术语

GB/T 32905—2016 信息安全技术 SM3密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4分组密码算法

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069—2010和GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

算法标识 algorithm identifier

用于对密码算法进行唯一标识的符号。

3.2

密钥派生函数 key derivation function

通过作用于共享秘密和双方都知道的其他参数，产生一个或多个共享秘密密钥的函数。

[来源：GB/T 25069—2010，2.2.2.124]

3.3

伪随机函数 pseudo random function

产生伪随机数的函数。

3.4

盐值 salt

作为单向函数或加密函数的二次输入而加入的随机变量，可用于导出口令验证数据。

[来源：GB/T 25069—2010，2.2.2.186]

注：盐值也称添加变量。

4 符号和缩略语

下列符号和缩略语适用于本文件。