ICS 35.040
CCS L 80

GM

# 中华人民共和国密码行业标准

GM/T 0093—2020

# 证书与密钥交换格式规范

**Certificate and key exchange format 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、西安西电捷通无线网络通信股份有限公司。

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、杜志强。

# 引　言

本文件的内容参照个人信息交换语法(RFC7292 PKCS ♯12),按照我国相关密码政策和规范,结合我国实际应用需求及产品生产厂商的实践经验,定义了基于SM2密码算法的证书与密钥交换格式。

对于需要传递的证书与密钥等用户个人信息,涉及信息机密性和完整性保护方法。机密性保护使用加密技术来防止个人信息被暴露,完整性保护则防止个人信息被篡改。

本文件支持机密性保护方法和完整性保护方法的四种组合。

所述机密性保护,有以下两种方法。

——公钥机密性保护方法:在源平台上,使用已知可信的目标平台的加密公钥以数字信封的形式来封装用户个人信息。这个数字信封可以被对应的加密私钥打开。

——口令机密性保护方法:用从机密性口令派生的对称密钥加密用户个人信息。如果同时使用口令完整性保护方法,机密性保护口令和完整性保护口令可以相同也可以不相同。

所述完整性保护,有以下两种方法。

——公钥完整性保护方法:通过对AuthenticatedSafe内容的数字签名来保证完整性。在源平台上,使用签名私钥产生数字签名。在目标平台上,使用对应的签名公钥来验证签名。

——口令完整性保护方法:通过保密的完整性口令产生消息鉴别码(MAC)来保证完整性。如果口令方式的机密性保护方法被同时采用,机密性保护口令和完整性保护口令可以相同,也可以不同。

注意,这里讨论的密钥仅指用于传递用户个人信息的密钥。用户可能希望把个人密钥从一个平台传递到另外一个平台(可以保存在PDU中),但不要将这里讨论的用于传递用户个人信息的密钥与用户的个人密钥混淆。

本文件通过基于公钥的机密性和完整性保护方法提供高层次的安全防护,需要源平台和目标平台分别具有可用于数字签名和加密的可信密钥对;同时也支持略低的安全需求,基于口令的机密性和完整性保护方法,用于不能提供可信密钥对的环境。

# 证书与密钥交换格式规范

## 1 范围

本文件规定了证书与密钥等信息的传递语法，包括私钥、证书、证书撤销列表、各种形式的秘密值及其扩展的标准化封装。

本文件适用于个人的SM2算法证书与密钥等信息在不同平台之间迁移的应用场景。

## 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—2012 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 35275—2017 信息安全技术 SM2密码算法加密签名消息语法规范

GB/T 35276—2017 信息安全技术 SM2密码算法使用规范

GB/T 33560—2017 信息安全技术 密码应用标识规范

GM/T 0091—2020 基于口令的密钥派生规范

GM/Z 4001 密码术语

## 3 术语和定义

GM/Z 4001和GM/T 0091—2020界定的术语和定义适用于本文件。

3.1

**属性 attribute**

一个ASN.1类型，标识一个属性类型(通过一个对象标识符)及其相关的属性值。

3.2

**平台 platform**

机器硬件、操作系统和应用软件组成的集合。

注：用户在这些环境中行使他的个人标识。在这里，应用是指使用用户个人信息的软件。如果机器硬件不同，或者软件不同，即为平台不同。在多用户系统中，每个用户至少有一个平台。

3.3

**源平台 source platform**

最终要传递到目标平台上的个人信息的起源平台。

3.4

**目标平台 target platform**

源平台上产生的个人信息要传递到的最终目的平台。

3.5

**目的加密密钥对 destination encryption key pair**

用于公钥机密性保护方法中的特定平台的密钥对。