ICS 35.040
L 80

中华人民共和国密码行业标准

GM/T 0067—2019

基于数字证书的身份鉴别接口规范

Interface specifications of authentication based on digital certificate

2019-07-12 发布　　2019-07-12 实施

国家密码管理局　　发 布

目　　次

前　言

本标准以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》为依据,规范了基于数字证书的身份鉴别密码应用接口。

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。

本标准由密码行业标准化技术委员会提出并归口。

本标准所使用的密码算法遵从国家密码管理主管部门公布的相关密码算法。

本标准主要起草单位:格尔软件股份有限公司、上海市数字证书认证中心有限公司、山东得安计算机技术有限公司、北京海泰方圆科技有限公司、成都卫士通信息产业股份有限公司、北京数字证书认证中心有限公司、国民技术股份有限公司、长春吉大正元信息技术股份有限公司。

本标准主要起草人:郑强、谭武征、韩玮、马洪富、蒋红宇、罗俊、傅大鹏、付月朋、赵丽丽。

基于数字证书的身份鉴别接口规范

1 范围

本标准规定了公钥密码基础设施体系上层应用中基于数字证书的身份鉴别接口。

本标准适用于公钥密码基础设施体系上层应用中身份鉴别服务的开发、证书应用支撑平台身份鉴别系统的研制及检测，也可用于指导应用系统规范化地使用证书进行身份鉴别。

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 15843.1—2017 信息技术 安全技术 实体鉴别 第1部分：概述

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

3 术语和定义

下列术语和定义适用于本文件。

3.1

证书认证系统 certificate authentication system

对数字证书的签发、发布、更新、撤销等数字证书全生命周期进行管理的系统。

3.2

证书撤消列表 certificate revocation list；CRL

由证书认证机构签发并发布的被撤销证书的列表。

3.3

证书验证 certificate validation

按照验证策略确认证书有效性和真实性的过程。

3.4

数字证书 digital certificate

也称公钥证书，由证书认证机构(CA)签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.5

用户凭证 identity token

能够表明用户身份的一段特定数据，用户通过向另一方提交此数据来表明自己的身份，此数据具有不可抵赖性和可验证性。

3.6

双向验证 mutual verify

向双方实体提供对方身份保证的实体鉴别。