ICS 35.040
CCS L 80

中华人民共和国密码行业标准

GM/T 0079—2020

可信计算平台直接匿名证明规范

Direct anonymous attestation specification for trusted computing platform

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：中国科学院软件研究所、国民技术股份有限公司、清华同方股份有限公司、北京华电卓识信息安全测评技术中心有限公司、兴唐通信科技有限公司。

本文件主要起草人：冯登国、秦宇、初晓博、张振峰、冯伟、赵世军、陈小峰、奚璨、杨糠、汪丹、刘鑫、郑必可、刘峰、张倩颖、常德显、刘韧、吴秋新、邵健雄、王微谨、杨波、张英骏。

可信计算平台直接匿名证明规范

1 范围

本文件规定了可信计算平台的直接匿名证明协议的功能、接口和数据结构。

本文件适用于可信计算平台直接匿名证明协议应用、匿名证明服务和匿名证明系统研发。

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 32918—2016(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GM/T 0012 可信密码模块接口规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的以及下列术语适用于本文件。

3.1

可信密码模块 trusted cryptography module;TCM

构建可信计算平台的基础硬件模块，为可信计算平台提供密码运算功能，具有受保护的存储空间。

3.2

签署密钥 endorsement key;EK

可信密码模块内部用于标识自身身份的密钥对，其用途只能用于加解密。根据上下文的不同情境，这个术语可能代表一个密钥对、密钥对中的公钥或者代表密钥对中的私钥。

3.3

TCM 服务模块 TCM service module

可信密码模块向应用程序提供服务的软件中间件。

3.4

直接匿名证明 direct anonymous attestation;DAA

可信计算平台所使用的匿名身份鉴别方案。

3.5

基于椭圆曲线的直接匿名证明 elliptic curve-based direct anonymous attestation

基于椭圆曲线密码学方案的直接匿名证明方案。

3.6

证明方 prover

直接匿名证明中的证明方，一般包含主机和可信密码模块两个部分。

3.7

主机 host

直接匿名证明中证明方拥有的内嵌可信密码模块的安全主机。