ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 40651—2021

信息安全技术　实体鉴别保障框架

Information security technique—Entity authentication assurance framework

2021-10-11 发布　　2022-05-01 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

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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：联想(北京)有限公司、国民认证科技(北京)有限公司、中国科学院数据与通信保护研究教育中心、中国科学院软件研究所、中国电子技术标准化研究院、格尔软件股份有限公司、中国信息通信研究院、北京国民安盾科技有限公司。

本文件主要起草人：柴海新、李俊、李汝鑫、吕娜、陈天宇、张严、郝春亮、郑强、宁华、傅山、沈明峰、顾小卓。

信息安全技术　实体鉴别保障框架

1　范围

本文件确立了实体鉴别的保障框架，规定了各参与方角色的职责、实体鉴别的主要流程环节以及实体鉴别保障等级的类别和等级划分原则，并规定了实体鉴别保障所需的管理要求。

本文件适用于实体鉴别服务的安全测试和评估，并为其他实体身份鉴别相关标准的制定提供依据和参考。

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 25069—2010　信息安全技术　术语

GB/T 35273—2020　信息安全技术　个人信息安全规范

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

断言　assertion

验证方生成的对实体进行鉴别的结果。

注：可能包含实体属性信息或授权信息等。

3.2

鉴别　authentication

用于对实体和其所呈现身份之间的绑定关系进行充分确认的过程。

3.3

鉴别器　authenticator

声称方拥有或掌握的可用于鉴别声称方身份的功能组件或方法。

注：鉴别器包含并绑定实体凭证或凭证生成方法，参与并执行特定的鉴别协议。

示例：密码模块、口令、口令生成器等。

3.4

鉴别协议　authentication protocol

在声称方和验证方之间定义的消息序列，使得验证方能够执行对声称方的鉴别。

3.5

鉴别因素　authentication factor

用于鉴别或验证实体身份的要素。

注：鉴别因素可分为三类：

——实体所拥有的事物（例如，设备签名、护照、包含凭证的硬件设备、私钥等），

——实体所知晓的信息（例如，口令、PIN 等），