ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36651—2018

信息安全技术　基于可信环境的生物特征识别身份鉴别协议框架

Information security techniques—Biometric authentication protocol framework based on trusted environment

2018-10-10 发布　　2019-05-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国科学院数据与通信保护研究教育中心、中国银联股份有限公司、联想(北京)有限公司、浙江蚂蚁小微金融服务集团有限公司、国民认证科技(北京)有限公司、北京数字认证股份有限公司、华为技术有限公司、三六零科技股份有限公司、中国信息通信研究院、数安时代科技股份有限公司、广州广电运通金融电子股份有限公司、北京旷视科技有限公司。

本标准主要起草人:荆继武、刘丽敏、回春野、杨楠、钱文飞、李俊、陈星、辛知、傅大鹏、常新苗、程斌、张屹、傅山、张永强、林冠辰、张鑫。

信息安全技术　基于可信环境的生物特征识别身份鉴别协议框架

1　范围

本标准规定了基于可信环境的生物特征识别身份鉴别协议框架，包括协议框架、协议流程、协议规则以及协议接口等内容。

本标准适用于生物特征识别身份鉴别服务的开发、测试和评估。

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 25069—2010　信息安全技术　术语

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

可信环境　trusted environment

用户设备上的安全区域，可保证加载到其内部数据的安全性，包括保密性、完整性和可用性等，如可信执行环境(TEE)、安全元件(SE)、可信密码模块(TCM)或其他具备安全边界的保护区域。

3.2

生物特征识别身份鉴别　biometric authentication

采用生物特征识别技术对用户的身份进行鉴别。

3.3

生物特征识别密钥管理器　biometric authentication key manager

负责维护身份鉴别服务器鉴别用户时需要的相关信息(例如密钥)的实体。

3.4

生物特征识别密钥管理器标识符　biometric authentication key manager identifier

用来标识生物特征识别密钥管理器，供身份鉴别服务器检索厂商公钥及生物特征识别密钥管理器相关信息。

3.5

用户设备　user device

包含生物特征识别密钥管理器的计算设备。

3.6

依赖方　relying party

依赖于其他实体(例如身份鉴别服务器)提供的关于用户的鉴别结果，对用户所使用的资源或者系统进行授权的实体。

3.7

应用程序标识符　application identifier

该标识符使用统一资源定位符表示，用来唯一标识依赖方的某一应用程序。