ICS 35.240.15
CCS L 70

中华人民共和国国家标准

GB/T 44285.1—2024

卡及身份识别安全设备　通过移动设备进行身份管理的构件　第1部分：移动电子身份系统的通用系统架构

Cards and security devices for personal identification—Building blocks for identity management via mobile devices—Part 1: Generic system architectures of mobile eID systems

（ISO/IEC 23220-1:2023,MOD）

2024-08-23 发布　　2025-03-01 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。

本文件是GB/T 44285《卡及身份识别安全设备　通过移动设备进行身份管理的构件》的第1部分。GB/T 44285已经发布了以下部分：

——第1部分：移动电子身份系统的通用系统架构。

本文件修改采用ISO/IEC 23220-1：2023《卡及身份识别安全设备　通过移动设备进行身份管理的构件　第1部分：移动电子身份系统的通用系统架构》。

本文件与ISO/IEC 23220-1：2023相比做了下述结构调整：

——本文件3.7“发现服务　discovery service”对应ISO/IEC 23220-1：2023中3.18的内容。本文件的3.8～3.18依次顺延对应ISO/IEC 23220-1：2023的3.7～3.17；

——本文件B.6对应ISO/IEC 23220-1：2023中B.5的内容。

本文件与ISO/IEC 23220-1：2023的技术性差异及其原因如下：

——用规范性引用的GB/T 35273和GB/T 40660替换了ISO/IEC 29100和ISO/IEC 19286(见5.2.1)，以适应我国的技术条件，增加可操作性。

本文件做了下列编辑性改动：

——增加了缩略语“TRE”(见第4章)；

——增加了B.5的内容。

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。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：中国电子技术标准化研究院、江苏赛西科技发展有限公司、深圳赛西信息技术有限公司、中移动金融科技有限公司、新大陆数字技术股份有限公司、北京安御道合科技有限公司、飞天诚信科技股份有限公司、北京中电华大电子设计有限责任公司、上海复旦微电子集团股份有限公司、深圳市雄帝科技股份有限公司、中关村芯海择优科技有限公司、大唐微电子技术有限公司、楚天龙股份有限公司、北京智芯微电子科技有限公司、东信和平科技股份有限公司、北京握奇数据股份有限公司、金邦达有限公司、武汉天喻信息产业股份有限公司、蚂蚁科技集团股份有限公司、北京眼神智能科技有限公司、深圳源明杰科技股份有限公司、北京华大智宝电子系统有限公司、中国邮电器材集团有限公司、上海浦东艾法金融科技身份认证技术创新中心、中国银联股份有限公司、兴唐通信科技有限公司。

本文件主要起草人：高健、蔡春水、果艳红、曹国顺、谢依夫、林冠辰、朱鹏飞、潘亮、张晖、郑嵩、何凡、李琨、白婧、楼水勇、赵轶、程文杰、黄海明、徐文军、蒋曲明、林靖、付英春、苏昆、杨春林、李延、王永涛、王昊、周吉天白、黎理明、王雪聪、钱涛、马立群、吴思捷、束敏、刘志强。

引　言

电子 ID 应用(eID 应用)通常用于具有集成电路的证章和 ID 卡,允许用户完成电子身份识别、鉴别或选择创建数字签名。许多不同的应用领域对这些机制都有基本需求,并使用不同的手段来提供这些功能(例如,人社系统有社保卡或医保卡,金融部门使用银行卡,政府部门有身份证、电子护照或驾照,教育系统有学生证或图书证,公司有员工卡,个人有会员卡等)。

移动设备(如移动电话或智能电话,可穿戴设备)是许多人日常生活的核心部分。它们不仅用于通信,还用于发送电子邮件、访问社交媒体、游戏、购物、理财,以及存储私人内容,如照片、视频和音乐。今天,它们被作为个人设备用于商业和私人应用。随着移动设备在日常活动中的无处不在,用户强烈要求在他们的移动设备上有电子身份应用程序(eID-Apps)或具有身份/鉴别机制的服务,即 mdoc 应用程序。

一个 mdoc 应用程序可以被部署来提供许多不同的数字 ID 证件。另外,它可以驻留在移动设备上的其他 eID 应用程序中。此外,用户可能拥有多个安装 mdoc 应用程序的移动设备,这导致了凭证和属性管理机制的增强。

部署 mdoc 应用程序的技术先决条件已经存在,它们被部分地标准化以支持移动设备上的安全和隐私。eID 应用程序解决方案的容器示例是基于软件的可信执行环境(TEE)、基于硬件的安全元件(如:通用集成电路卡(UICC)、嵌入式或集成式 UICC(eUICC 或 iUICC)、嵌入式安全元件、带加密模块的安全存储卡[19]或其他驻留在移动设备上的专用内部安全装置),以及具有基于服务器安全手段的解决方案。

由于 mdoc 应用程序可以位于具有不同安全手段的不同形式的移动设备上,它们尽可能地通用,以便能够被不同的可信 eID 管理变体所采用。这种多样性也导致了不同级别的安全、信任和保证。因此,可信的 eID 管理意味着(远程)管理和使用一个或几个安全元件(例如,以智能网络的形式)、凭证和用户属性,并具有适合其能力和力量的不同安全级别。

外部世界对 mdoc 应用程序的访问通过可用的传输通道进行。典型的本地信道为二维条码扫描、BLE、近场通信(NFC)和 WLAN 等,而远程通信通常为通过移动网络和 WLAN 网络的互联网联接。身份识别方式和传输接口及协议的选择是可信的 eID 管理的重要部分。

mdoc 应用程序被用于日常生活的不同领域,是不同标准化活动的重点。本文件旨在提供其他标准可使用的机制和协议,以提供互操作性和互换性。考虑到这些基本情况,未来的 mdoc 应用程序可以衍生,并可能扩展 GB/T 44285。

GB/T 44285 建立在现有标准的基础上,包括四个主要特点:

a)　安全通道建立;

b)　API 调用序列化方法;

c)　数据元素命名约定;

d)　通信信道协议上的有效载荷传输。

此外,它还增加了建立首次使用信任(TOFU)的手段。

注:GB/T 44285继承并增强了移动驾驶执照应用所采用的功能,从而确保与ISO/IEC 18013-5的向后兼容性。

GB/T 44285《卡及身份识别安全设备　通过移动设备进行身份管理的构件》拟分为以下六个部分。

——第 1 部分:移动电子身份系统的通用系统架构。目的是确定系统通用架构和应用相关流程。

——第 2 部分:移动电子身份系统的数据对象和编码规则。目的是确定系统通用的数据格式,以

便于交换。

——第3部分:安装发行阶段的协议和服务。目的是规定发行阶段的协议和服务。

——第4部分:运行阶段的协议和服务。目的是规定运行阶段的协议和服务。

——第5部分:信任模型和可信度评估。目的是规定可信模型和信任等级。

——第6部分:对安全区的可信度进行认证的机制。目的是确定使用安全区可信度认证的机制。

卡及身份识别安全设备　通过移动设备进行身份管理的构件　第1部分：移动电子身份系统的通用系统架构

1　范围

本文件规定了基于移动 eID 系统的基础设施构件组成的通用系统架构和通用生存周期，同时规范了 mdoc 应用程序和移动验证应用的接口和服务。

本文件适用于参与移动 eID 系统的规范、架构、设计、测试、维护、管理和运行的实体。

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 35273　信息安全技术　个人信息安全规范

GB/T 40660　信息安全技术　生物特征识别信息保护基本要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

属性　attribute

用户属性　user attribute

实体（3.6）的特征或特性。

示例：实体类型、地址信息、电话号码、权限、MAC 地址、域名都是可能的属性。

[来源：ISO/IEC 24760-1：2019，3.1.3]

3.2

属性声明　attribute statement

描述用户属性（3.1）的声明或断言，包括对属性的谓词。

[来源：ISO/IEC 19286：2018，3.6]

3.3

鉴别　authentication

为实体（3.6）的身份（3.11）提供保证。

[来源：ISO/IEC 29115：2013，3.2]

3.4

鉴别协议　authentication protocol

实体（3.6）和验证者（3.40）之间定义的消息序列，使验证者能够对实体进行鉴别（3.3）。

[来源：ISO/IEC 29115：2013，3.4]