ICS 25.040.01
CCS N 10

T/CAMETA

中国机电一体化技术应用协会团体标准

T/CAMETA 001050—2025

网银U盾数字化管理方法与技术规范

Digital management methods and technical specifications for online banking U-Shield

征求意见稿

2025－04－01 发布

2025－07－01 实施

中国机电一体化技术应用协会　　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这些专利的责任。

本文件由中国机电一体化技术协会提出并归口。

本文件起草单位：中国铁建股份有限公司、中核汇能有限公司、新华水力发电有限公司、厦门新同事科技有限公司、北京众合云科集团有限公司等。

网银U盾数字化管理方法与技术规范

1 范围

本文件界定了网银U盾数字化管理方法及技术规范的术语和定义，规定了网银U盾数字化管理规范的总体要求、岗位与职责设置、实物安全管控规范和安全使用规范，数字化管理系统的技术架构、服务器设备技术规范、权限管控平台技术规范、数字化操作客户端软件技术规范、集成开发接口规范和数字化管理机房技术要求。

本文件适用于企业资金结算部门、财务共享服务中心、人力资源共享服务中心的大规模U盾数字化安全管控系统建设、日常管理及运维工作。

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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25000.51—2016 系统与软件工程系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

GB/T 32400—2015 信息技术 云计算 概览与词汇

GB/T 41778—2022 信息技术 工业大数据 术语

GB 50174—2017 数据中心设计规范

3 术语和定义

GB/T 32400—2015、GB/T 41778—2022界定的以及下列术语和定义适用于本文件。

3.1

网银U盾 online banking U shield

为确保网上交易的保密性、真实性、完整性和不可否认性，采用非对称密钥算法对网银交易身份数据和业务数据进行加密、解密和数字签名的内置微型智能卡处理器，是企业办理网上银行业务的电子签名、数字认证的USB电子身份证。也称：第一代网银U盾。

3.2

第二代网银U盾 the Second Generation online banking U shield

在第一代网银U盾基础上，增加了交互式操作按钮，以及可实时显示交易关键信息的，通过计算机屏幕外实体按钮的交互确认操作来确保交易安全性液晶显示屏的网银U盾。

3.3

网银支付制单 online banking payment voucher preparation

企业网银业务系统填报付款方开户名称、账号、银行名称，收款方开户名称、账号、银行名称，支付金额、支付理由等基本支付信息数据的过程。

3.4

网银支付审核 online banking payment review

在企业网银业务系统，审核并确认制单环节所填报数据与支付数据的一致性，最终确认并同意支付的过程。

3.5

网银U盾权限 permissions for online banking U shield

企业网银业务系统赋予每个网银U盾使用者查询、制单、审核、二次审核等操作权限。

3.6

网银U盾服务器 USB server for online banking U shield

通过智能USB-HUB、嵌入式操作系统、虚拟USB驱动软件功能模块组合，对网银U盾进行集中管理并向客户端计算机提供U盾连接和使用服务的智能硬件产品。

3.7

权限管控平台 permission control platform

能够对网银U盾基础台账、U盾使用者账号等基础数据进行安全管理，并能够对U盾使用者进行权限分配、使用行为记录和追溯的管理软件。

3.8

网银U盾操作客户端软件 client software for U shield operation

引导网银U盾使用人员以数字化方式获取U盾使用权的应用软件。

3.9

应用程序编程接口 application programming Interface(API)

网银U盾管理系统向其他应用软件开发平台所提供的,用于实现U盾操作的一系列可直接调用的函数。

4 数字化管理规范

4.1 总体要求

基于网银U盾服务器、权限管控平台、网银U盾使用客户端软件所搭建的管理系统，对网银U盾进行人盾分离、权责到人的数字化管理方法；应能实现网银U盾可用而不可及的技术效果，实现网银U盾使用行为“事前有记录、事中有记录、事后可追溯”的管理效果。

4.2 岗位权限与职责

4.2.1 数据管理员

数据管理员岗位权限与职责如下：

a) 收集网银 U 盾及其网银账户基础台账；

b) 在权限管控平台维护网银 U 盾及网银账户基本数据；

c) 在网银 U 盾服务器为网银 U 盾分配安装位置；

d) 及时清除已撤出 U 盾的基础数据。

4.2.2 权限管理员

权限管理员岗位权限与职责如下：

a) 创建 U 盾使用者账户；

b) 配置 U 盾使用者账户安全属性；

c) 为 U 盾使用人员分配和创建权限列表；

d) 在 U 盾使用人员岗位变更、临时休假期间进行权限转移和委托变更；

e) 对于离职或调岗人员，及时停用或删除其使用人员账号；

f) 基于交叉监督机制，对其他权限管理人员创建的权限进行审批确认。

4.2.3 U 盾实物管理员

U盾管理员岗位权限与职责如下：

a) 设置至少 2 名 U 盾实物管理人员；

b) 实物管理人员只能拥有机房门禁或网银 U 盾保险柜单一门锁开门权限；

c) 实物管理员可由数据管理员兼任。

4.2.4 网银支付制单员

网银支付制单员岗位权限与职责如下：

a) 能够被分配查询类和制单类网银 U 盾使用权；

b) 能够通过客户端软件的人机交互界面，连接制单类 U 盾办理网银支付制单业务。

4.2.5 网银支付审核员

网银支付审核员岗位权限与职责如下：

a) 能够被分配查询类和审核类网银 U 盾使用权限；

b) 能够通过客户端软件的人机交互界面，连接审核类 U 盾办理网银支付审核业务。

4.2.6 RPA 机器人数字员工

RPA机器人数字员工岗位权限与职责如下：

a) 能够依据 RPA 机器人流程执行需求，分配查询、制单或审核类 U 盾使用权限；

b） 能够通过 API 接口，在权限控制下连接和使用 U 盾，模拟人工办理网银业务。

4.3 U 盾实物安全管控规范

4.3.1 基本原则

4.3.1.1 人盾分离

人盾分离原则主要包括：

a） 将 U 盾使用权与保管权分离；
b） 网银 U 盾集中存放于网银 U 盾服务器；
c） 网银 U 盾服务器安装于安全保险柜；
d） U 盾使用人员通过专用客户端软件，在权限控制下数字化调用网银 U 盾。

4.3.1.2 先授权后使用

任何U盾使用者只能在被授权且授权被审批确认的前提下，才能拥有网银U盾使用权；未经特殊许可，不得将网银U盾从安全保险柜撤离后离线使用。

4.3.1.3 交叉监督

交叉监督原则主要包括：

a） 机房门禁、网银 U 盾保险柜开锁密钥，应安排不同专人保管，建立两人以上交叉监督的安全机制，确保 U 盾实物安全性。
b） U 盾保险柜支持密码或生物特征识别开锁的安全机制；密码长度不得低于 8 位数字字符；密码错误重试次数超过 5 次后，应暂时锁定账户操作。

4.3.2 U 盾外借与归还

特殊情况下需外借U盾的，需要在公司内部OA系统发起审批；经业务负责人审批核准后，打印审批单，交由U盾实物管理人员从机房取出U盾，并在权限管控平台进行登记。登记信息包括：外借人员姓名、外借用途、外借时间、预期归还时间等基本信息。

4.3.3 U 盾实物盘点

U盾实物盘点原则主要包括：

a） 推荐至少每月进行一次 U 盾实物盘点，也可按需进行盘点；
b） 每次盘点时，建议统计每个 U 盾的如下基本信息：
U 盾可用性、关联开户账户、开户名称、授权使用人、与上次巡检对比（新增、外借、无变化）、证书截至日期等信息。

4.3.4 安防与预警

U盾实物管理人员与财务部资金结算管理人员，可通过视频监控等手段，实时查看网银U盾实物存放位置的实况录像；布防期间，未经审批的非法闯入人员，在触达U盾保险柜之前，即可向管理人员发出报警信息。

4.4 U 盾安全使用规范

4.4.1 U 盾使用授权与审批

U盾使用授权与审批应遵循以下要求：

a） 指定至少两位权限管理人员负责权限管理，实现权限分配与权限审批相互独立；
b） 由权限管理人员根据任务分工创建 U 盾使用权，由其他权限管理人员进行权限确认审批；
c） 支持权限互斥机制，同一网银账户的制单与审核类 U 盾使用权，不能分配给通过一位 U 盾使用人员；
d） 建立交叉监督机制，权限列表创建与审批人员不能是同一人。

4.4.2 U 盾使用权限变更

U盾使用权限变更应遵循以下要求：

a） U盾使用人员岗位变更或临时请假，可通过权限变更授权其他业务人员使用U盾；

b） 权限变更包括权限的转移和临时委托两种模式；

c） 权限变更可由业务人员自行发起，经由一位权限管理人员审批确认后生效；

d） 权限变更应具备明确的有效期，有效期时间结束，权限自动失效。

4.4.3 使用人员身份识别

使用人员身份识别应遵循以下要求：

a） 按照等级保护三级系统要求，对制单、审核类U盾，需采用双因子安全策略对U盾使用人进行身份校验。

b） 推荐采用账号密码方式登录客户端软件；对制单、审核等带有支付权限的U盾，每次连接U盾或发送按压确认键时，通过计算机屏幕外的技术手段进行身份校验。例如，基于生物特征识别或电子围栏等快捷高效的身份校验方式，以提升工作效率。

c） 网银U盾数字化管理平台，建议配置网银U盾使用者离岗检测能力，U盾使用者离岗时，自动断开已连接U盾并锁定计算机屏幕，以提升安全性。

4.4.4 网银U盾使用

应支持多种方式快速检索并选择网银U盾数据，通过“连接”、“断开”等操作按钮，快速获取和释放U盾使用权；支持相互协作的多位U盾使用者在无需管理员介入的情况下，相互转移U盾使用权。

4.4.5 U盾证书有效期管理

至少每月一次，对网银U盾证书到期时间进行盘点，对已到期、本月到期、次月到期网银U盾进行续期操作，避免证书过期无法办理网银业务。

5 数字化管理系统技术规范

5.1 系统技术架构

5.1.1 系统架构图

网银U盾数字化管理系统，由网银U盾服务器、安全保险机柜、权限管控平台、客户端软件、身份校验终端设备等组成，网银U盾服务器，安装到安全保险机柜内；权限管控平台、网银U盾服务器，以及客户端软件所在计算机，通过内部网络设备建立连接；身份校验终端通过USB总线、串行总线等方式连接到客户端计算机。典型系统架构如图1所示：

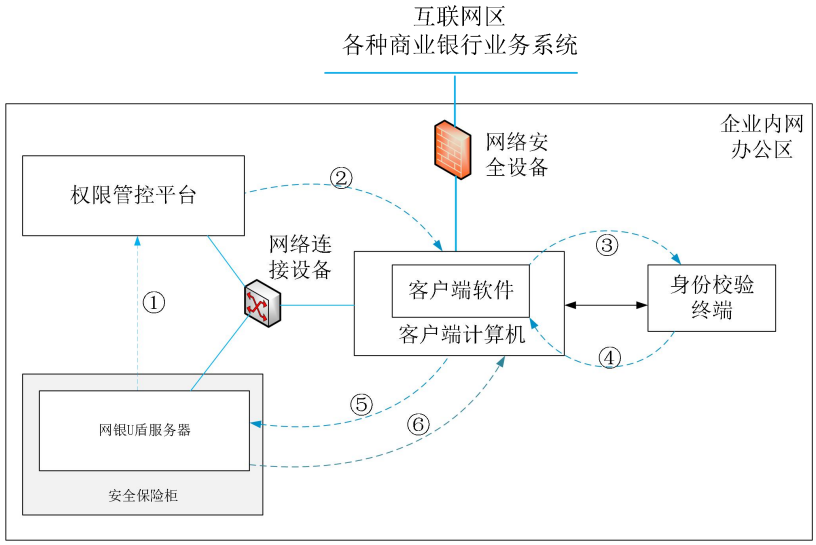

图 1 系统架构图

5.1.2 工作流程

典型技术架构的核心安全策略在于，客户端软件每次发起网银U盾操作时，先请求身份校验终端校验操作人员身份，身份校验通过后生成“不可伪造、不可复制、不可篡改”的单次有效的Token，客户端软件携带该Token向U盾服务器发送操作命令，确保网银U盾的使用过程安全受控。各工作环节工作流程如下：

a) 网银 U 盾服务器向权限管控平台注册，并实时反馈自己的工作状态；
b) U 盾使用人员通过客户端软件，从权限管控平台查询其授权列表；
c) 客户端软件向身份校验终端请求身份校验；
d) 身份校验终端向客户端反馈身份校验结果，以及单次有效的 Token 信息；
e) 客户端软件携带 Token 信息请求 USB 服务器映射 U 盾使用权；
f) 网银 U 盾服务器向客户端软件映射 U 盾使用权。

5.2 服务器设备技术规范

5.2.1 基本原理

网银U盾服务器与客户软件是本系统的核心组成部分，其基本原理如**错误！未定义书签。**所示。“服务端虚拟USB驱动程序”将网银U盾数据转换为TCP/IP协议数据转发送给“客户端虚拟USB驱动程序”；“客户端虚拟USB驱动程序”将收到的TCP/IP数据还原为网银U盾数据，等效于在客户端计算机插入该网银U盾。

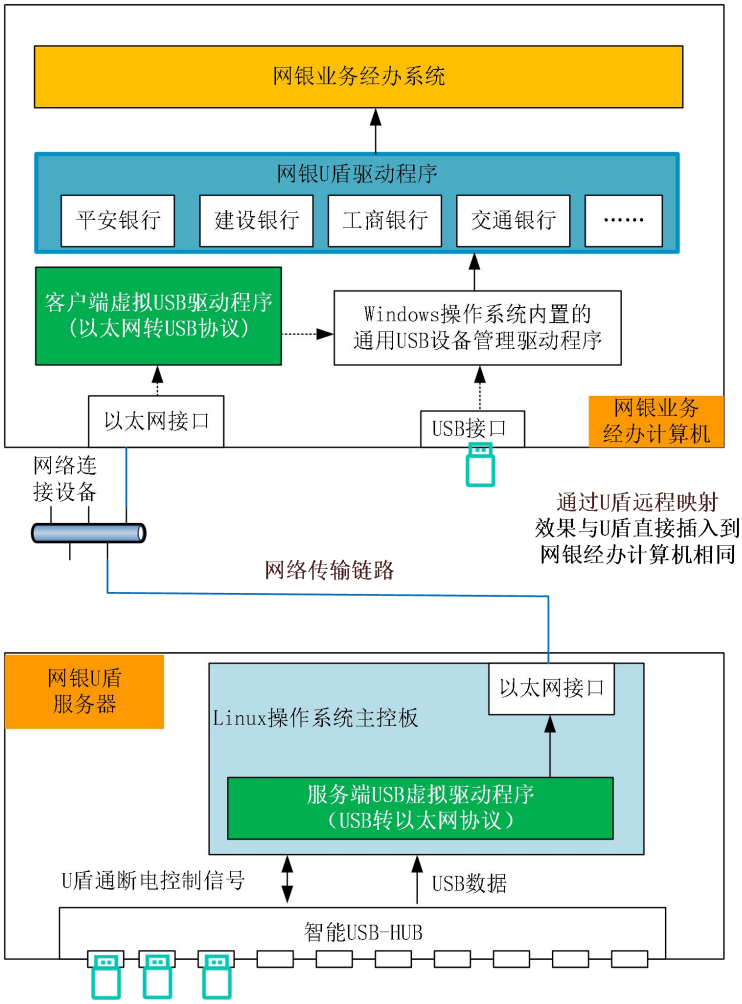

图 2 服务器技术原理图

5.2.2 结构形式

网银U盾服务器包含一套智能USB-HUB，用于管理网银U盾，以及由中央处理器（CPU）以及嵌入式服务器操作系统组成的控制核心。对于第二代网银U盾，还应包含有能够承载U盾的安装模块，安装模块具备能够按压U盾确认键的机械臂。U盾安装模块应采用模块化架构设计，具体要求如下：

a) 每个 U 盾安装模块，可以独立地从 USB 服务器内置导轨拔出，实现免工具装卸和维修保养，方便财务人员自行装卸 U 盾；
b) 每个 U 盾安装模块，通过连接件直接连接到智能 USB-HUB，以确保 USB 信号传输稳定性，从根本上消除导致系统性风险的技术隐患；
c) 每个 U 盾安装模块，具备双面接触的防滑机制，避免 U 盾滑动而无法按压确认键；
d) 每个 U 盾安装模块，支持在线热插拔维护更换，无需专业人员、无需任何工具即可拆卸更换；
e) 每个 U 盾安装模块，内置机械臂控制系统，能实现表面按压、侧向按压和尾部按压三种操作形式。

5.2.3 安装形式

应设计合理的安装结构。应适应小规模部署桌面安装形式和满足大规模集群化部署的机柜安装形式：

a) 桌面安装形式，须为网银 U 盾服务器配置带有安全锁具的保险柜；
b) 保险柜安全锁具优先推荐配置具有指纹或密码等身份校验能力的安全锁具。

5.2.4 安全防护

每个USB连接端口应具备短路、过压、过流、过热保护能力；插入异常的网银U盾，不会损坏设备；网银U盾服务器异常时，不会损坏正常的U盾；特别注意，要求保护能力应具备自恢复能力，异常条件排除后，能够自动恢复正常功能。应具备15kV以上的防静电能力，防止装卸U盾时因静电损坏USB-HUB控制电路板。

5.2.5 初始状态

每个USB端口应独立控制通电、断电；每个网银U盾端口，应采用按需通电策略，无业务办理时，应处于断电保护状态。

5.2.6 网络接口

应优先推荐配置2个以上的千兆网络连接接口。

5.2.7 电源接口

220V两相三线制供电，输入电压范围110V～250V，应支持国标或欧标电源输入线。

5.2.8 核心配件

CPU等核心配件，应采用国产化低功耗CPU，无风扇静音设计，在办公室场景下运行时不会干扰影响业务人员正常工作。

5.2.9 安全认证

应内置CPU、操作系统，通过网络连接为客户端提供U盾连接和使用服务，且工作电流小于6A，符合国家对强制质量认证的服务器产品定义要求；优先推荐采用通过CCC强制认证的USB服务器类产品。

5.3 权限管控平台技术规范

5.3.1 架构形式

权限管控平台应采用以下技术架构形式：

a) 优先推荐采用 B/S 架构形式设计；
b) 服务端支持集群化高可用企业级架构部署模式；
c) 服务端支持业务服务与数据库服务相互分离；
d) 数据库支持主从模式的自动备份机制。

5.3.2 运行环境

5.3.2.1 网络环境

应采用企业内部网络私有化部署方式，配置必要的网络安全设备禁止任何外部访问。

5.3.2.2 硬件环境

应兼容支持所有国产信创认证的硬件平台。

5.3.2.3 操作系统

应兼容支持国产信创认证的操作系统。

5.3.2.4 数据库环境

应兼容支持国产信创认证的数据库环境。

5.3.3 功能模块

应采用数据管理、权限管理、系统配置三权分立的原则，不同角色允许访问不同页面。

5.3.3.1 系统配置

权限管控平台系统配置应满足以下要求：

a) 创建数据管理员、权限管理员账户；
b) 配置本单位工作日历，实现节假日控制；
c) 配置 API 接口密钥，实现系统集成的安全管控。

5.3.3.2 设备监控

应可以监控和查看所有设备运行状态、每个端口的通电、断电状态。

5.3.3.3 数据管理

数据管理应满足以下要求：

a) 将 U 盾数据与网银账号数据分别建立台账，能满足单一 U 盾关联多个网银账户“超级盾”的管理要求。
b) 可单个添加，也可以基于模板批量导入数据，将 U 盾与设备端口绑定；
c) 可单个添加，也可以基于模板批量导入数据，将网银账号与 U 盾绑定。

5.3.3.4 权限管理

权限管理至少包括：用户管理、角色配置、权限编辑、权限审批四个子模块。

a) 用户管理子模块，创建 U 盾使用人账户列表，支持绑定计算机 MAC 地址，防止越权登录；
b) 角色配置子模块，配置使用人员角色，自动批量分配 U 盾使用权；
c) 权限列表子模块，可查看每一位使用者的全部 U 盾使用权，并对权限进行追加、删除、转移、委托、修改有效期等操作；
d) 权限审批子模块，确保两人以上共同确认，才能改变 U 盾使用权，达到交叉监督的效果。

5.3.3.5 日志管理

应以结构化形式记录每一次U盾使用行为，能够记录的行为类型包括：连接U盾、断开U盾、按键操作、权限创建、权限转移、权限委托、权限确认、权限删除等。

5.3.4 安全设计

5.3.4.1 安全设计

应按GB/T 22239—2019、GB/T 28448—2019的规定进行安全设计；

5.3.4.2 测试验证

应按GB/T 25000.51—2016的规定进行测试验证。

5.3.4.3 技术安全策略

技术安全策略应按以下规定进行：

a) 应对登录用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；比如，密码长度不得低于 8 位，包含数字、字母、特殊符号的组合；密码建议 3 个月更换一次。
b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；例如，当日密码输错次数达到 5 次，锁定登录账号；
c) 应采取 SM3\SM4 等国密算法，对身份确认信息进行加密，具有必要的措施防止鉴别信息在网络传输过程中被复制、伪造和篡改；
d) 应采用动态口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。例如，推荐采用账号密码+短消息口令验证码相结合的方式；
e) 网银 U 盾使用者账户，允许强制绑定 MAC 地址，防止非法越权登录；
f) 其他技术安全策略应符合 GB/T 25000.51—2016 的要求。

5.3.4.4 数据安全策略

数据安全策略应按以下规定进行：

a) 应采用校验技术保证权限管控平台用户信息和网银 U 盾使用者关键信息,例如用户账号及密码数据、权限配置数据等重要个人信息等，在传输过程中的完整性。
b) 应采用校验技术保证权限管控平台用户信息和网银 U 盾使用者关键信息,例如用户账号及密码数据、权限配置数据等重要个人信息等，在存储过程中的完整性。
c) 采用分布式加密存储与备份机制，数据库服务故障后可在 8 小时内恢复关键数据。

5.3.5 安全测评认证

应能通过GB/T 25000.51—2016的安全测评。

5.4 数字化操作客户端软件技术规范

5.4.1 技术架构

应包含驱动层的虚拟USB总线驱动软件和应用层的客户端操作软件。

5.4.2 驱动层软件技术规范

5.4.2.1 核心软件

虚拟USB总线驱动软件属于网银U盾数字化管理系统的核心软件，应优先推荐国产自研、源代码可控的软件产品。

5.4.2.2 控制指令

虚拟USB总线驱动软件与网银U盾服务器核心软件之间的控制指令,应采用私有密钥加随机数进行加密，确保指令不能被复制、篡改和伪造。

5.4.3 客户端操作软件技术规范

客户端操作软件建议采用C/S架构。

5.4.4 主要功能列表

5.4.4.1 身份校验

客户端操作软件应具有健全的身份校验机制，确保U盾使用人是被授权本人。按GB/T 22239-2019中对等级保护三级系统的技术要求，应采用包含动态口令、账号密码、短消息、生物特征、电子围栏等多种身份校验方式中，至少两种以上的校验方式。为充分平衡操作效率与安全性，建议在不同的场景下采用如下身份校验组合：

a) 固定工位办公，建议登录客户端软件采用账号密码方式校验身份，连接使用 U 盾时，采用指纹或电子围栏相结合的方式校验身份；
b) 移动工位办公，建议登录客户端软件采用账号密码方式校验身份，连接和使用 U 盾时，采用电子围栏方式校验身份；
c) 临时出差场景，建议登录客户端软件采用账号密码方式校验身份，连接和使用 U 盾时，采用短消息方式校验身份。

5.4.4.2 查询显示授权列表

客户端操作软件支持通过开户银行名称、网银账号、开户名称等多种关键字进行查询并显示当前用户的权限列表。

5.4.4.3 连接并使用 U 盾

在客户端软件的U盾数据列表中，选择一条U盾数据点击“连接”按钮，客户端软件应该先进行身份校验，确保身份校验有效后，再请求身份校验终端生成单次有效的Token令牌，客户端凭该Token向网银U盾服务器发送U盾映射命令，并获取U盾使用权。

5.4.4.4 释放 U 盾使用权

在客户端软件的已连接U盾列表中，选择一条U盾数据点击“断开”按钮，客户端软件向网银U盾服务器发送断开U盾映射命令，并释放U盾使用权。

5.4.4.5 按压 U 盾确认键

在客户端软件的U盾数据列表中，选择一条U盾数据点击“按键操作”按钮，客户端软件应该先进行身份校验，确保身份校验有效后，请求身份校验终端生成单次有效的Token令牌，客户端凭该Token向网银U盾服务器发送按压U盾确认键的命令。

5.4.4.6 网银 U 盾数据维护管理

能够导出自己所负责网银U盾数据，并将网银U盾按照证书有效期分类，包括已过期、本月到期、次月到期等网银U盾，方便业务人员按计划处理U盾证书续期工作。

5.5 集成开发接口规范

集成开发接口，用于允许RPA机器人、其他财务管理软件等通过API集成开发接口使用U盾。

5.5.1 API 接口功能范围

集成开发接口应至少包含：查询U盾状态、连接、断开、发送确认键命令等功能。

5.5.2 API 接口身份校验

应对API调用者创建U盾使用者账号，并为其分配U盾使用权限。API接口应当身份校验机制，确保API接口调用过程不可复制、不可篡改、不可伪造。

5.6 数字化管理机房技术要求

5.6.1 门禁

应当由不同人员保管，实现相互监督的安全机制对U盾实物进行安全管控。门禁的配置应符合以下要求：

a) 数字化管理机房，应配置账号密码、口令、生物特征识别能力的门禁系统；
b) 保险柜也应配置账号密码、口令或生物特征识别能力的门禁系统。

5.6.2 安全监控

U盾管理房间应配置具备人体行为分析能力的摄像头，当检测到未经授权的越权闯入时，向管理员发送报警信息。

5.6.3 温湿度控制

按GB 50174—2017的要求，进行温湿度控制。网银U盾管理设备应配置良好的动态环境监控系统，建议室内温度控制在18～27℃之间；湿度范围推荐在20%～80%之间。

参 考 文 献

[1] GB 4943.1—2022 音视频、信息技术和通信技术设备 第1部分：安全要求
[2] GB/T 9254.1—2021 信息技术设备、多媒体设备和接收机 电磁兼容 第1部分：发射要求
[3] GB 17625.1—2022 电磁兼容 限值 第1部分 谐波电流发射限值（设备每相输入电流≤16A）
[4] GB/T 43697—2024 数据安全技术 数据分类分级规则

《网银 U 盾数字化管理方法与技术规范》

编制说明

一 工作简况

（一）项目来源

由中国铁建股份有限公司、厦门新同事科技有限公司等向中国机电一体化技术应用协会提出立项申请，经立项（中机电协标〔2024〕第4号），并在全国团体标准信息平台公示（https://www.ttbz.org.cn/Home/WebDetail/85555），项目名称：《网银U盾管理系统技术标准》。

（二）项目背景

2021年3月2日，国务院国资委发布《关于加强中央企业资金内部控制管理有关事项的通知》，要求各中央企业内控部门要建立资金内控关键要素管理台账，对网银U盾及其责任人等关键要素进行限时备案管理。

（三）发展阶段

网银U盾是企业法人、社会团体实现资金支付的身份凭证。加强网银U盾管理，是财务领域“加强资金监管”重要组成部分。

传统的网银U盾管理，都是采用人工分散线下管理方式，U盾实物管理、使用过程监管、使用行为跟踪缺乏技术手段。管理过程尚未实现数字化，已经成为财务数字化升级中的薄弱环节。

网银U盾管理系统发展经历了以下几个阶段：

1、第一阶段：人工线下管理各种U盾。

网银 U 盾产品自 2003 年开始伴随着电子银行的出现开始在企业内使用。

根据 U 盾在网银的不同操作权限，分为查询 U 盾、制单盾和审核盾等不同类型。

早期网银 U 盾都是由企业资金结算部门手工线下管理。不同权限类型 U 盾由不同的专人负责，人工进行借还等级保管。

2、以 USB 智能集线器管理查询类 U 盾。

2018 年前后，RPA 机器人开始在国内财务共享分为中心推广，通过 RPA 机器人自动下载网银流水并实现自动对账，率先提出了网银 U 盾的数字化管理和使用需求。

由于 RPA 场景只关心 U 盾的基础连接能力，核心需求是能够以数字化手段连接和使用 U 盾，USB 智能集线器产品能够很好地满足了使用需求，开始在财务共享服务中心推广。

3、以网银 U 盾服务器产品管理制单审核类 U 盾。

2020 前后随着国务院国资全面推进委对司库建设；2021 年 3 月，国资委发文要求企业建立健全资金安全核心要素监管能力。企业财务共享中心开始将网银 U 盾智能化管理作为一项基础能力建设。这个阶段的典型特征是：对数字化管理系统提出了更好的安全要求，比如具备双因子安全身份校验能力确保 U 盾使用过程的安全性；具有先进的硬件结构，确保规模化部署无系统性风

险。

二 目的意义

网银U盾智能管理是企业资金安全核心要素管理能力提升的着力点和实际抓手。

探索网银U盾的先进管理方法，以数字化、智能化手段提升网银U盾管理的安全性，也是近年来财务数字化、智能化转型的迫切需求。

本标准拟对行业内先进经验进行总结推广，为更好地提升网银U盾管理工作贡献力量。

三 标准制定原则和编写规则

（一）制定原则

在科学理论和实践经验基础上，确保技术要求和规范具有科学性和可行性，能够有效指导实际施工过程。标准编制坚持一下原则：

1、统一性原则：标准编制坚持统一各方的要求，确保项目参与单位能够按照该标准进行操作、实施，具备可行性。

2、公正性原则：编制过程坚持公正、公平、透明，确保标准的制定过程中各方利益的平衡，不偏袒任何一方，保证标准的

客观性和公信力。

3、可操作性原则：编制时充分考虑实际操作性，确保项目参与单位能够对照标准的要求实施，避免过于理论化或难以实施的情况。

4、合规性原则：编制符合国家法律法规和相关行业的规范和标准，确保标准的合法性和合规性，遵循国家政策和法律要求。

（三）编写规则

标准起草工作小组本着全面、科学、合理、实用的原则进行本文件的制定工作。根据行业现状和生产技术需求，结合实际生产情况，做到优化、量化、细化，维护标准的协调与统一。充分考虑理论和实践依据，兼具广泛性、适宜性和可操作性，兼容并包。文件编写按 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》的规定进行：

1、统一性：对涉及的术语进行定义，明晰引用文件术语定义的适用情况，以确保所有相关人员对标准的理解和应用具有统一性，避免因理解差异导致的执行偏差。

2、协调性：严格遵循现行的相关法律、法规和强制性国家标准，避免标准体系内部各部分之间的冲突、重复。

3、适用性：在编制过程中，充分考虑应用场景的多样性，确保标准应具有足够的灵活性，以适应不同环境下的具体需求。

4、一致性：文本结构、逻辑一致，行文及相关描述清晰无歧义。

5、规范性：遵循规范化的制定流程，以确保标准的科学性、公正性和权威性。

四 标准制定工作概况

（一） 标准制定相关单位及人员

1、本文件归口单位：中国机电一体化技术应用协会。

2、本文件主要起草单位：厦门新同事科技有限公司等。

（二） 主要工作过程

1、2024年3月～5月，成立标准化工作小组，完成前期准备、前期市场调研、资料收集统计分析。

2、2024年6月～7月，形成初稿报中国机电一体化技术应用协会进行立项。

3、2024年8月～10月，完成收集资料的讨论，提出相关技术指标和参数，形成标准草案进行讨论，组织相关企业召开研讨会。

4、2024年11月～2025年4月，针对研讨会的意见和建议，修改形成征求意见稿。标准征求意见稿、编制说明发至全国团体标

准信息化平台（www.ttbz.org.cn）、检测机构、大专院校、同行企业、征求意见。

5、2025年5月，收集、整理全国团体标准信息化平台（www.ttbz.org.cn）、检测机构、大专院校、同行企业所征求的反馈意见，形成送审稿。

6、2025年5月，针对收集的到的征求意见和建议，邀请行业专家完成技术评审。

7、2025年6月，针对专家评审会提出的意见和建议，修改完善形成正式报批稿。

8、2025年7月，编写发布公告，并至全国团体标准信息化平台（www.ttbz.org.cn）发布，联系出版社组织出版，组织标准的宣贯实施。

五 适用范围和主要技术内容

（一） 适用范围

界定网银U盾数字化管理方法及技术规范的术语和定义，规定网银U盾数字化管理规范的总体要求、岗位与职责设置、实物安全管控规范和安全使用规范，数字化管理系统的技术架构、服

务器设备技术规范、权限管控平台技术规范、数字化操作客户端软件技术规范、集成开发接口规范和数字化管理机房技术要求。

适用于企业资金结算部门、财务共享服务中心、人力资源共享服务中心的大规模U盾数字化安全管控系统建设、日常管理及运维工作。

（二） 主要技术内容

通过明确适用范围、限定内容、信息安全、实施模式管理办法、智能化内容、成果形式等基本规定；通过技术架构、核心软件技术参数、硬件安全技术标准、电磁兼容标准、接口结构技术规范、远程按压确认键技术规范等设备技术标准，技术实现架构、数据安全、使用安全策略研究、权限分配技术策略、使用过程日志记录、日志查询与统计分析等数据与权限管控平台技术标准，远程调用操作方法、身份校验、安全策略方法、实物安全管控方法、服务器的U盾管理方法、日常运维与制度等研究。制定出符合财务数字化领域网银U盾管理方法技术规范和运维制度规范。主要技术指标及内容有:

3 术语和定义

4 数字化管理规范

4.1 总体要求

4.2 岗位权限与职责

4.3 U 盾实物安全管控规范

4.4 U 盾安全使用规范

5 数字化管理系统技术规范

5.1 系统技术架构

5.2 服务器设备技术规范

5.3 权限管控平台技术规范

5.4 数字化操作客户端软件技术规范

5.5 集成开发接口规范

5.6 集成开发接口规范

六 与现行相关法律、法规、规章及相关标准的协调性

（一） 目前国内主要执行的标准

无。

（二） 本文件与相关法律、法规、规章、强制性标准相冲突情况。

无冲突情况。

（三） 本文件引用的文件

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25000.51—2016 系统与软件工程系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

GB/T 32400—2015 信息技术 云计算 概览与词汇

GB/T 41778—2022 信息技术 工业大数据 术语

GB 50174—2017 数据中心设计规范

引用文件现行、有效。

（三） 本文件参考的文件

GB 4943.1—2022 音视频、信息技术和通信技术设备 第1部分：安全要求

GB/T 9254.1—2021 信息技术设备、多媒体设备和接收机电磁兼容 第1部分：发射要求

GB 17625.1—2022 电磁兼容 限值 第1部分 谐波电流发射限值（设备每相输入电流≤16A）

GB/T 43697—2024 数据安全技术 数据分类分级规则

七 重大分歧意见的处理经过和依据

本文件在起草过程中，没有产生重大分歧。

八 贯彻标准的要求和措施建议

标准起草单位将在企业标准信息公共服务平台（https://www.qybz.org.cn/）上自我声明采用本文件，其他采用本文件的单位也应在相应信息平台上进行自我声明。

九 其他应予说明的事项

本文件制定过程中，未发现本文件涉及专利和知识产权的问题。

团体标准标准起草工作小组

2025年4月