阿谱斯网银管控系统安全白皮书

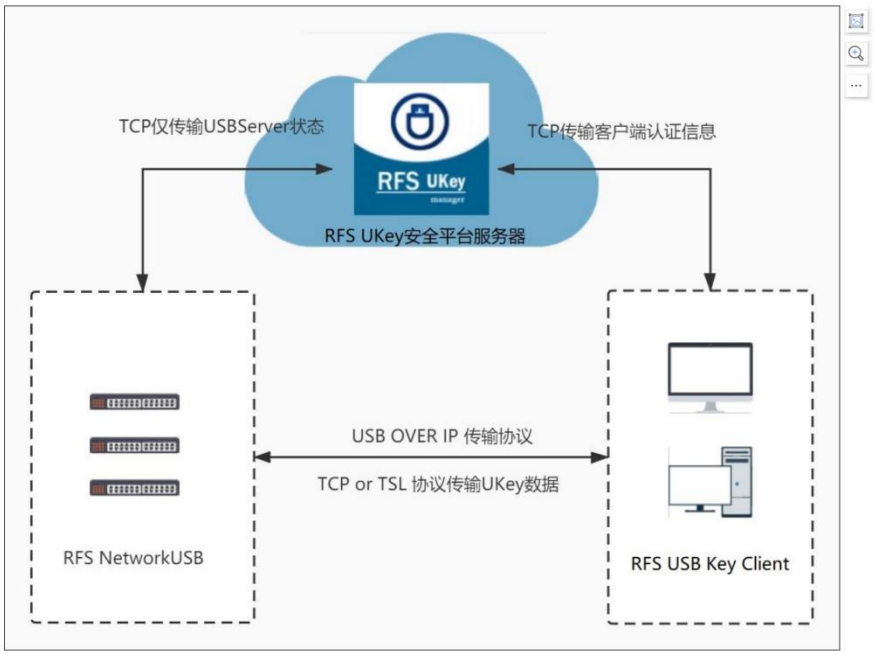
一．产品安全性解析

1. 整体系统架构安全性

阿谱斯 UkeyManger 安全管控系统采用：U 盾接入设备内网部署+软件平台私有化部署的标准企业级安全架构。做好内外网隔离，外网无法访问设备及软件平台，有效对外网攻击进行屏蔽，最大程序减少网络共计风险。

同时软件平台部署在客户内网自建服务器上，U 盾集中插在专用智能 USB hub 上，设备只是通道，不存储任何用户敏感信息（包括网银账号及网银密码）。资金业务员安装 RPUSI 客户端软件，经账密验证及通过平台管理员授权后使用 U 盾。登录网银时，网银密码通过银行网银控件加密通信保护，同时不存储于系统及资金电脑中，亦不会留痕，不存在网银密码丢失风险。

系统架构图



阿谱斯 UkeyManger 安全管控系统采用的该架构确保用户数据安全的同时，即便设备故

障维修或平台软件维护时，也不会造成客户信息泄露。

（反之，如一些竞品如厦门 XXX，北财 XXX 等，采用依靠单台 U 盾接入设备里内置软件进行 U 盾管理，没有私有化部署的管控平台软件，则会存在以下数据安全风险：

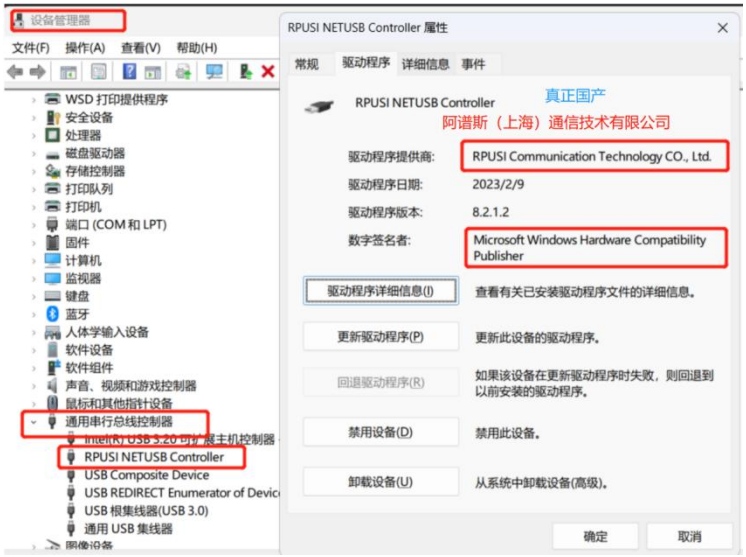
功能简单：限于单台 U 盾接入设备的硬件性能，存储控件及计算能力，U 盾管理软件功能简单单一，数据存储时效短（如 U 盾使用日志），管理超过 100 枚 U 盾后，还会造成系统卡顿，数据丢失。

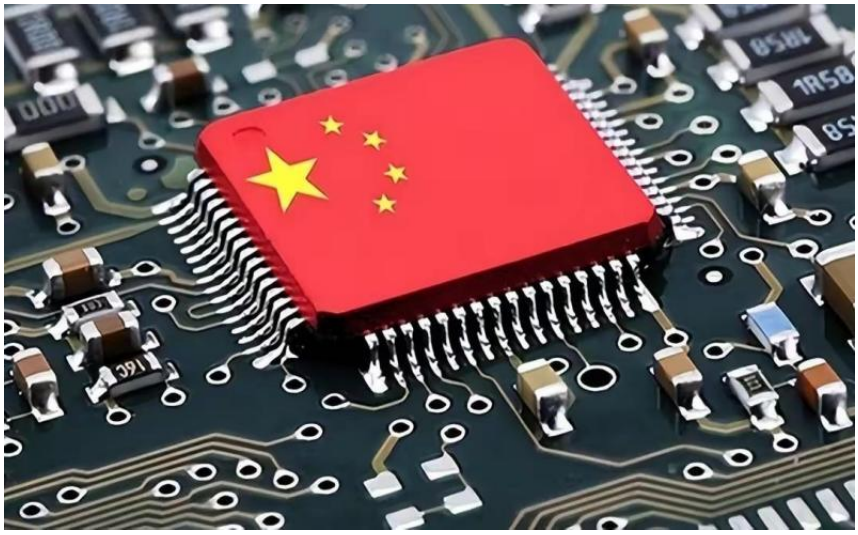
数据泄露：最为关键的是，用户的关键数据，如资金业务人员的客户端账号密码，网银盾的机密信息，以及使用权限等等，都存储于 U 盾接入设备上，一旦设备出现故障，则整个系统的管理能力瞬间瘫痪，使得系统崩溃无法使用；故障返修时，系统不但无法使用，且用户的关键数据在返修过程中被厂商“轻而易举的获取”。

网络风险不可控：这台 U 盾接入设备是整个系统中最关键，但网络防护能力又不可控的部位，受限于 USB 服务器的网络防风险性能，它并没有强大的网络防护能力，处于网络攻击中的薄弱环节，一旦这个管理节点 USB 服务器出现系统漏洞或网络后门，则其中的关键信息和用户数据很容易被网络攻击非法获取，后果严重不可想象！）

2. 国产信创自主可控

阿谱斯的 USB HUB 设备的底层驱动程序、客户端软件、管控平台、按键矩阵等全部为国产自主研发，有完整软著专利等相关知识产权，最为核心的 U 盾连接的驱动程序为自主研发，非第三方国外授权取或破解版驱动程序。平台软件可在国产化多种操作系统上部署运行。不存在被国外企业后门远控或切断服务问题。





RPUSI 阿谱斯通信 Connect Automation

KYLINSOFT 麒麟软件

麒麟软件适配认证

阿谱斯（上海）通信技术有限公司

阿谱斯UKey安全管控平台 V5.10

与

麒麟软件有限公司

银河麒麟高级服务器操作系统（飞腾版）V10

银河麒麟高级服务器操作系统（鲲鹏版）V10

完成兼容性测试，能够达到通用兼容性要求及性能、

可靠性要求，满足用户的关键性应用需求

特此颁发适配认证

阿谱斯（上海）通信技术有限公司

麒麟软件有限公司

适配认证专用章

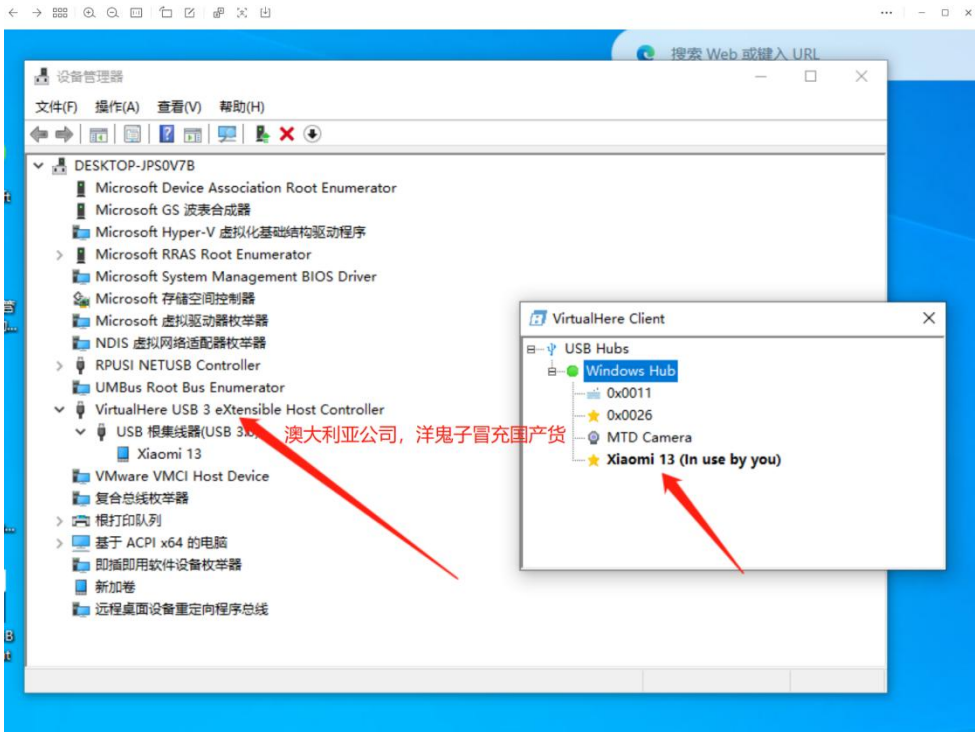
在线查验证书

证书编号：20250320S-009

2025年03月20日

"麒心伙伴"计划

阿谱斯的 USBHUB 设备核心 CPU 及元器件等均采用国产工业级 ARM 处理器，满足全国产化要求。而如一些竞品设备，使用普通电脑主板加 USB 扩展卡改装而成，采用国外 CPU 芯片；同时没有能力自研驱动程序，驱动程序采用国外或第三方 USB OVER IP/USB IP 软件，有如澳大利亚 Vitualhere 的授权软件（北 XXX），Fabula Tech 驱动程序（北京盛 XXX），上海某个人工作室 Drivercoding 驱动程序伪装成自有的 CLOUDUSB（厦门 XXX），存在知识产权纠纷的风险，且有随时被停用的巨大风险或存在严重信息泄露和安全风险。



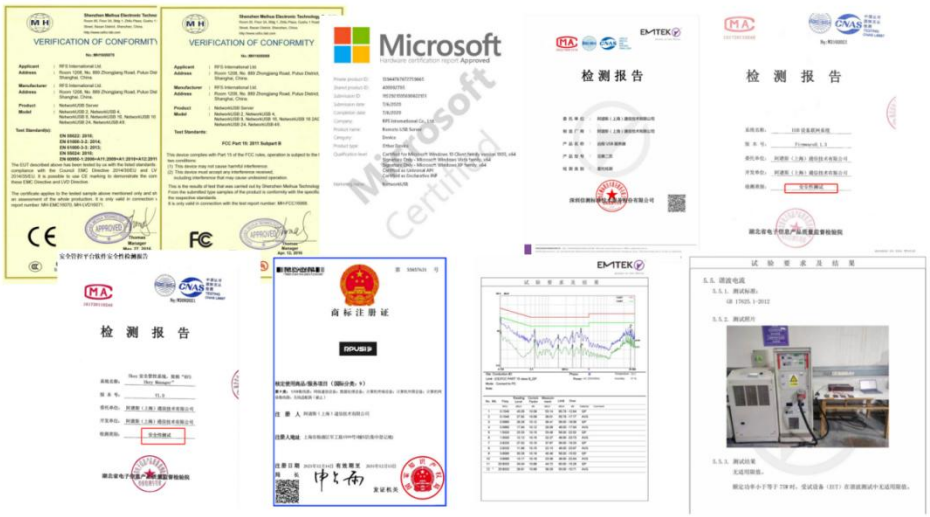
3. 国家认可的第三方安全检测认证报告

阿谱斯硬件设备、软件均有国家认可的第三方安全检测报告或证书，硬件可提供 CCC、FCC\CE 等电气安全报告，软件可提供国家认可的第三方扫测及安全评估报告。

设备有严格的安全设计，如端口 15KV 静电保护、设备采用医疗级安全电源等；

软件有严格密码保护、数据加密传输等机制，采用 RSA 算法及 TSL1.2/1.3 算法加密；

特别是 UUBHUB 等硬件设备，大部分客户没有专用独立机房，将设备放置在财务室或设备间；阿谱斯设备采用嵌入式设计，对环境温湿度适应性高；电磁兼容通过国家标准的检测，对人体无影响健康环保；U 盾部署专用安全机柜采用加密锁，辅助监控设备，机箱物理锁，出入口门禁等手段全方位对 U 盾进行有效保管。



二. 产品安全性功能解析

1. 阿谱斯 U 盾管控平台科学严格的安全管理功能

阿谱斯 Ukey manager 安全管控系统软件，有严格的 U 盾安全管理机制，确保用户核心网银资产安全使用。

从业务风控角度看，核心安全理念是：U 盾使用必须是经过事先授权后，方可根据 U 盾属性和账户身份属性进行合规使用，杜绝过去靠人为约束使用 U 盾；

- ✓ 可创建多维度管理员账号，管理员可按机构分划管理 U 盾及人员范围，或自定义功能范围，如经办盾管理员，复核盾管理员，系统查询管理员，资金业务员账号管理员，权限分配管理员，可有效做到专人专职，杜绝单一管理员权限过大；
- ✓ 系统有复杂密码及安全码等登录认证机制，强制使用复杂密码，定期密码修改提醒；
- ✓ U 盾分级授权机制，如经办、复合、管理盾需对应资金用户相应类型才可分配 U 盾使用权限；
- ✓ 资金业务员严格按系统授权权限使用 U 盾（账户只能看到和操作自己被授权过的 U 盾）；
- ✓ 可设置使用 IP 地址白名单访问；
- ✓ 可启用单点登录安全模式（绑定资金业务员电脑与客户端账号，换电脑不允许登录使用）
- ✓ 可设置 U 盾使用审批机制（某些重要 U 盾，可通过软件平台/企业微信/钉钉等设置使用通知或审批，经审批方可连接 U 盾）
- ✓ 有完整的登录使用日志供事后审计（管控平台会记录所有使用 U 盾连接断开使用日志，但无法也不能记录登录网银后的行为）
- ✓ 有异常报警日志供审计（同一账户在不同电脑登录，不同账号在同一电脑登录，更换 U 盾，设备掉线等异常报警日志）
- ✓ U 盾与设备端口绑定，提醒并禁止设备端口换 U 盾套取非法使用权限，设备更换 U 盾必须重新入库及分配授权；
- ✓ 实时在线监测所有 U 盾在用状态，包括当前使用人，及使用人电脑 IP，以及使用起始时间；
- ✓ 平台具备 U 盾远程盘点、统计功能，可实时盘点系统内 U 盾数量，物理位置及使用情况；

2. 资金岗 U 盾使用安全机制

按用户账号进行 U 盾权限分配：每个资金业务岗需管理员给其创建使用账号，管理员通过给用户账号分配 U 盾，用户客户端登录后可使用管理员所分配的 U 盾，未分配给其的 U 盾则无法使用。

密码保护功能：账号密码有高复杂性设置（如长度必须大于 8 位、必须含 3 种符号和密码修改频率），同时可自定义到期更换密码提醒。U 盾使用软件账号密码，资金业务岗人可在使用软件上自行修改并加密同步至管理端，管理员无法查看及获取。

单点登录功能：如资金业务岗的客户端账户设置了单点登录功能，则账户与该人员的办公电脑进行绑定，无法使用别的电脑登录 U 盾使用软件。

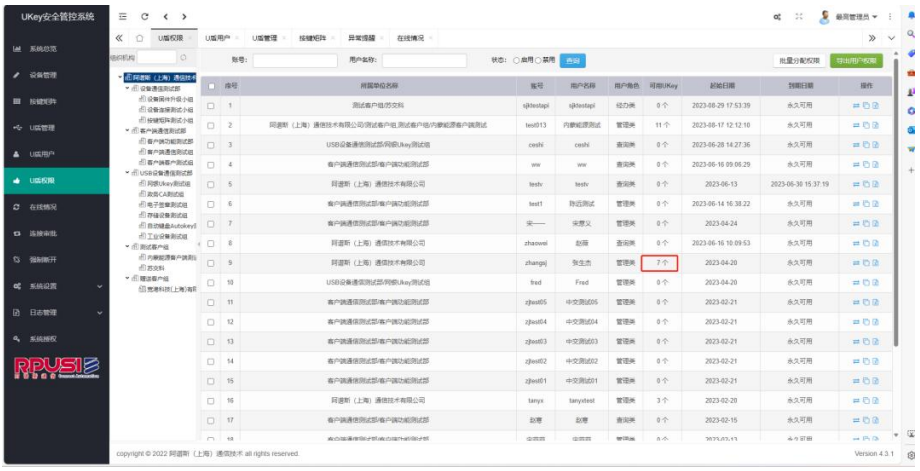
连接密码功能：每一枚 U 盾，管理员可设置独一无二的连接密码，在业务员登录使用软件后，连接某一 U 盾时，仍需输入正确的连接密码后，系统方可开放连接功能；配合系统多位管理员交叉管控功能，如数据管理员只负责录入 U 盾及连接密码，权限管理员只负责分配 U 盾使用权限，则可最大限度降低操作风险。即：资金岗用户需要使用 U 盾，需先验证客户端软件账号密码，再验证某一 U 盾的连接密码后才能连接该 U 盾，再需验证网银的账户密码后方可进入网银页面。3 层无关联的密码验证机制，加上密码加密存储传输，以及网银控件对网银密码得有效防护，使用 U 盾如在保险柜中一般。

U 盾连接及审批：每一枚 U 盾，管理员都可根据重要性单独设置是否使用通知及是否审批，若开通通知功能，则业务岗人员使用这枚 U 盾时，管理员在管控平台界面及企业微信等地收到连接通知，包括使用人名称，电脑 IP，时间等；若开通审批功能，则业务岗人员使用这枚 U 盾时，必须通过管理人员临时审批后，才可连接使用。

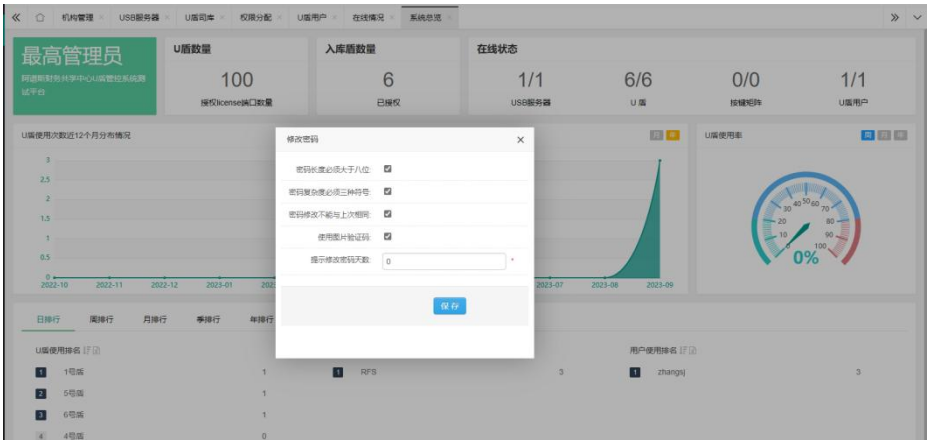
日志记录功能：平台会记录用户登录、使用 U 盾的时间和管理员的操作日志，并且有异常报警（如设备网络掉线及 U 盾过期提醒）日志供审计。

客户端登录多因子验证功能：客户端软件，及资金岗人员使用 U 盾的软件，需要通过有效的账号密码登录，同时可开启动态验证码校验。亦或选择在资金岗电脑上接入指纹识别模块，选择验证账号密码的同时，同时验证资金岗人员指纹后才可登录并使用 U 盾。指纹数据必须通过本地的指纹识别模块识别验证，无法伪造，进一步确保安全。

管理平台页面



密码强度设置页面



3. 多管理员 U 盾管理隔离及分级授权机制

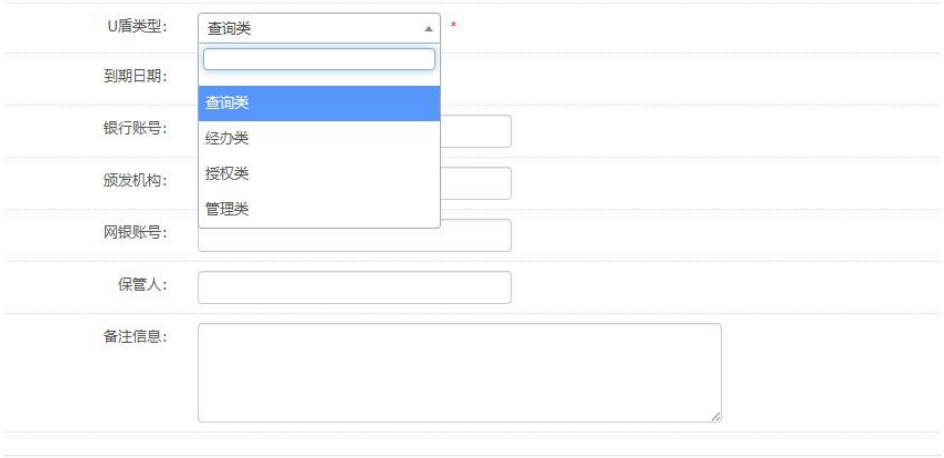
多样管理员交叉管理：阿谱斯 Ukey manager 安全管控系统可创建多级机构树，可将 U 盾分别划入不同机构或分组中，如按开户主体划分，或按类型划分。系统同时可创建多位管理员单一管理指定机构或分组，实现 U 盾的隔离管理。如经办盾数据管理员只管理经办盾数据录入，及经办盾权限管理员只负责经办盾权限分配；复核盾数据管理员只管理复核盾数据录入，及复核盾权限管理员只负责经办盾权限分配，做到权限分隔，缩小风险范围。

同时可另设资金岗用户管理员，用户管理员负责创建资金岗账户，不参与权限分配及 U 盾管理；权限管理员只负责分配权限，无法新建资金岗用户并分配 U 盾使用权至新用户下。

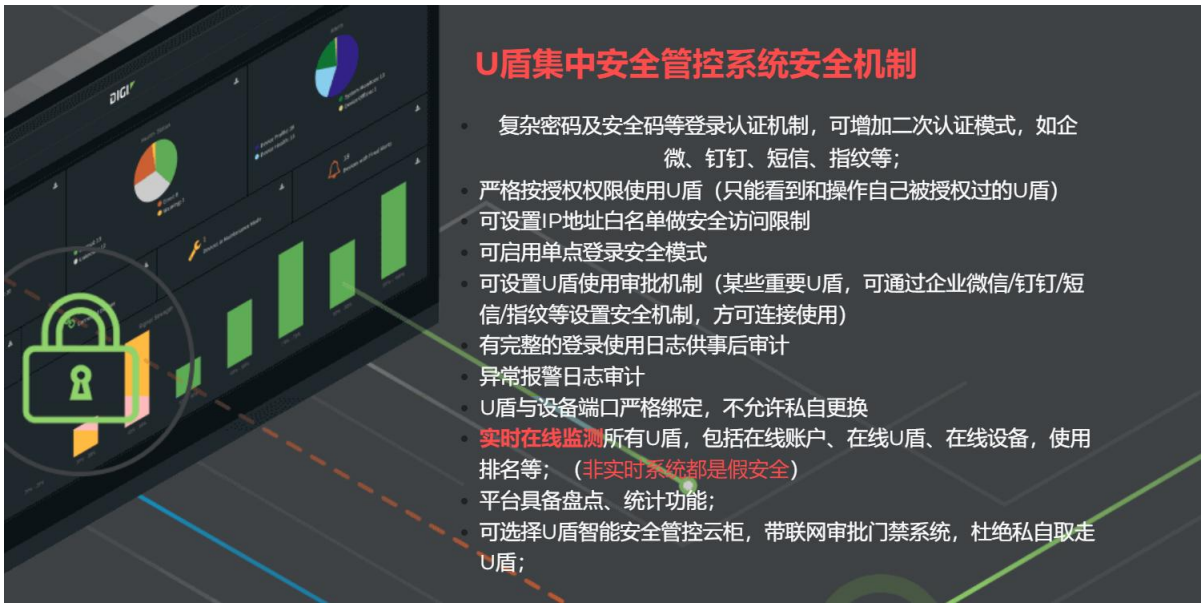
U 盾分级授权机制：U 盾录入入库时可对其类型进行设置：查询、经办、授权、管理类，级别依次递增。创建用户账号时也必须设置账号类型（查询、经办、授权、管理类），用户

的账号类型和 U 盾类型对应；权限分配管理员只能严格按 U 盾类型及资金岗用户类型严格分配 U 盾使用权，例如账号类型是经办类，则无法分配和使用授权类和管理类的 U 盾，同时该管理无权修改 U 盾类型及资金岗用户类型。

U 盾类型设置



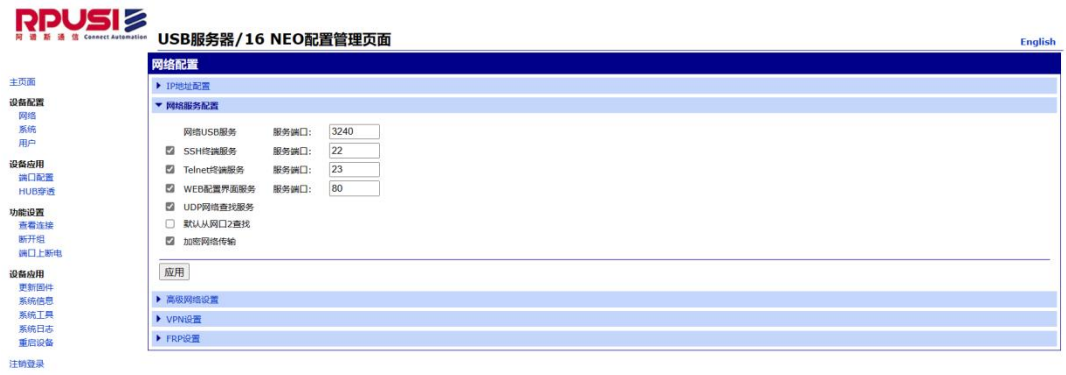
U 盾分配页面，棕色代表账号权限不足无法分配

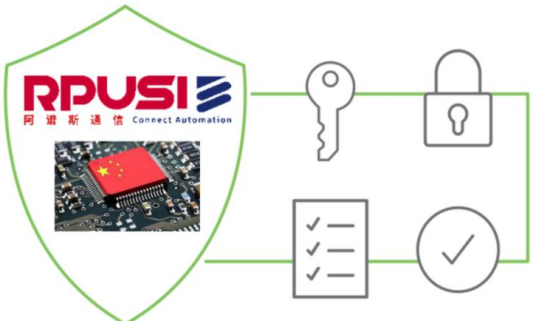


4. 智能 USB HUB 安全机制功能

端口访问控制：在 NetworkUSB 服务器 web 页面，端口配置—USB 端口连接控制配置页面，可以对整台设备或 USB 端口（组）进行安全访问限制。添加允许接受的 IP，或者拒绝接受的 IP。此功能可设置该台设备或 USB 分组只允许特定的 IP 或 IP 段地址主机连接使用。

数据安全传输设置：TSL 加密传输方式，保证数据通信安全





NetworkUSB设备安全相关机制及申明

- 国产自主可控，满足信创要求，国产CPU，核心底层驱动程序完全自研
- 正规IT设备，非电脑改装拼凑伪设备合
- 正规国家认可的第三方型式试验检测报告
- 电气特性安全，如电磁兼容性、15KV ESD端口保护、电源安全、接地安全等
- 无中高危网络漏洞
- 数据带加密传输SSL,TLS；访问带安全码机制及设置IP白名单
- 设备结构安全，防尘、防鼠、防虫全密闭设计
- 网络访问端口可更改
- 可有选择性地关闭开启一些服务，如SSH、HTTP
- 满足等保三级要求
- 支持国产信创操作系统，如麒麟
- 可设置安全码进行安全验证后连接

总结：

阿谱斯通信 USBHUB 及安全管控系统通过多维度安全机制，实现以下安全要素：

- ✓ 网银 U 盾数据及权限隔离管理；
- ✓ 多方管理员交叉管理及制约；
- ✓ U 盾得安全合规使用，多因子账户验证；
- ✓ 人盾分离，严格授权使用；
- ✓ U 盾使用日志记录、异常报警记录；
- ✓ U 盾实时使用通知及临时审批；
- ✓ U 盾库实时状态监控、物理位置监测、U 盾盘点统计等全流程管控；

阿谱斯 UkeyManger 安全管控系统针对大型财务共享中心，全方位多维度的 U 盾管控，及严格使用权分配审批，账户多因子验证等有效的安全机制，得到大量央企国企等高安全要求客户的认可和选择。

阿谱斯（上海）通信技术有限公司
www.remoteusb.com
021 -52688815