

摘要【300-320，不要超过330】：

2023年11月份，我所在公司承担了某银行“智能终端管理系统”的开发工作，我作为该项目的系统架构设计师，负责该系统的需求分析与架构设计工作。该系统**主要提升银行对智能收银终端软硬件的管理及维护能力**，业务模块包括应用APP管理、设备管理、远程协助以及屏媒广告等。本文以该平台为例，论述系统安全架构设计在该项目中的具体应用。本文首先重点论述鉴别框架和访问控制框架在该项目中的设计，以及如何提升平台的安全性。其次说明在项目实际开发过程中，存在的问题以及解决方案。整个项目历时11个月开发完成并顺利上线，到目前运行稳定。该系统也凭借着其卓越的安全性能和用户体验，赢得了行方一致的好评，通过这一实践，深刻体会到了系统安全架构设计在现代系统研发中的重要性。

正文【2200-2500】：

随着互联网技术的飞速发展，传统的收银设备操作系统简单，功能单一，无法远程升级（OTA），设备的状态也无从得知，所以智能设备替换传统收银设备是一个趋势。为了增加商户的粘性，提升服务质量，各大银行开始加大智能收银终端的投放。不同于传统的收银设备，智能设备联网能力强，操作系统强大，能够实现更多更复杂的业务。为了充分发挥智能设备的优势，并进一步提高银行对设备的监管，行方提出建设一个智能终端管理系统的需求，实时监控设备状态，并对设备的软硬件生命周期进行有效的管理。

2023年11月份，我司承担了某银行的智能终端管理系统的开发工作，我作为该项目的系统架构设计师，参与整个开发过程。该系统的主要业务模块包括应用APP管理、设备管理、远程协助以及屏媒广告等。建设该系统旨在加大银行对设备的管理，提升对商户设备的监管能力，以及对设备的维护效率。应用APP管理模块，主要包括应用上架，应用管理等功能。银行或商户可定制专属应用市场，上传和发布自己的APP。银行作为管理方，还可以针对不同业态的商户配置应用的可见性。设备管理模块，包括设备总览、定制设备以及远程更新功能。银行通过平台的可视化界面，能够清晰、实时的关注到设备当前的软件使用情况和硬件状态。另外，银行可通过平台配置装机初始化任务，设备首次激活时，会联网获取装机任务，包括定制开机动画、应用预装以及系统配置等。远程协助模块，主要包括文件传送接送，录屏以及远程控制等功能。针对软件常见的BUG问题，在商家授权后，通过该平台的远程协助功能，可远程操控设备，获取设备日志，便于软件开发人员排查问题。屏媒广告模块，主要包括媒体资源管理、广告数据统计等功能。银行或商户可通过平台上传广告资源，如优惠活动宣传等，并分析广告播放的数据统计。

银行对于安全性极为重视，在需求初期特别强调了安全性的重要性，并要求将安全性作为整个项目的核心目标之一。我通过引入先进的安全设计理念和技术手段，力求在系统的每一个层面都构建起坚固的安全防线，以抵御来自各个方面的安全威胁。这一举措不仅提升了平台的整体安全性，也为公司在领域的持续发展奠定了坚实的基础。接下来我会详细介绍该项目的实施过程。

1、鉴别框架

鉴别框架在智能终端管理系统中主要负责验证登录者的身份，确保只有合法的用户才能访问授权的资源，比如设备信息、用户信息以及系统软件信息等。鉴别框架设计内容较为复杂，涵盖了多个方面。首先在鉴别机制上，该智能终端管理平台采用了多种鉴别机制，除了传统的用户名密码方式，还增加了短信动态令牌机制，有效抵御了密码猜测和重放攻击等常见安全威胁；其次在鉴别协议上，它保证了鉴别过程中信息的机密性和完整性，该智能终端管理平台采用了先进的加密技术和安全协议，如TLS/SSL，确保信息通讯过程中数据不被截获或篡改；最后在鉴别信息管理上，因为对于密码要求较为严格，所以我们采用了哈希算法对密码进行摘要计算存储，实施细粒度的访问控制策略，并且定期要求用户修改密码，防止泄露。

同时，鉴别框架的应用在智能终端管理系统中也存在多种安全威胁及潜在的危害。比如，社会工程学攻击类型，恶意攻击者可能伪装成系统的技术支持人员，骗取用户的敏感信息，如登录密码、动态令牌等。再比如，数据泄密，恶意的软件入侵或人为的操作失误，都有可能导致数据的泄露。

1. 访问控制框架

访问控制框架在该系统中主要用于控制不同等级的用户对系统资源的访问，只有合法的用户才能访问对应的系统资源，从而保证了业务安全。首先，我们针对银行和商户的角色区分，制定了详细的访问控制策略，包括明确用户角色、权限和资源之间的关系，以及实现基于角色的访问控制（RBAC）等机制。在该系统中，区分银行和商户两类用户，针对银行还区分各级行的角色，每个角色在系统中的权限是不同的。如商户只能查看自己的应用商店，自己的设备信息，而支行或分行可以查看自己机构下商户的全部设备、应用信息。通过RBAC机制，杜绝了用户的越权访问情况。其次，我们还设计了访问控制模型，常见的访问控制模型包括自主访问控制，强制访问控制等。在该系统中，将自主访问控制应用在用户对自身创建的资源的访问，如商户可以查看自己上架的应用信息。而强制访问控制，则应用在敏感信息的场景，针对敏感性较高的数据，比如设备数据，只有特定权限的管理员才能访问。

智能终端管理系统通过访问控制框架制定了严格的访问控制机制，但也仍然存在着一些安全威胁和潜在的危害。如内部威胁，权限较高的用户利用自身权限能力，可能会恶意的进行数据的非法篡改，甚至破坏系统的安全。另一方面，用户因为自身缘故，不小心删除了重要数据，导致系统安全漏洞，进而影响平台的正常运行和用户的数据安全。

从鉴别机制方面来看，随着新兴技术的飞速发展，未来将有更多的认证方式出现，这对于平台鉴别机制设计要保证足够灵活，能够应对未来更多认证方式的导入。关于该问题，我们采用了插件化和模块化设计的来构建鉴别框架，每个认证方式都被设计为独立的模块或插件，因为耦合度低，提高了框架的扩展性和可维护性。

从访问控制框架方面来看，目前系统中已存在的用户就包含各级行的用户角色以及商户，权限又各有不同，所以访问控制模型的建立也要充分考虑到未来可能出现的更多角色或权限的引入。针对该问题，我们引入了基于属性的访问控制模型（ABAC），来实现更细粒度的访问控制策略，该模型允许我们基于用户属性、环境条件等多维度的权限判断，比RBAC具备更高的灵活性和安全性。

整个项目历时11个月开发完成，并于2024年10月顺利上线，到目前运行稳定，市场反馈良好。实践证明，通过基于此架构设计的智能终端管理平台，不仅提升了系统的安全性和易用性，同时，系统在大规模设备管理中展现出了良好的稳定性，有效提升了银行智能终端管理效率，减少了设备维护成本，从项目完工后的使用效果来看，达到了预期目的，也获得了行方的一致好评。

最后，经过这次参与系统安全架构设计实施后，我也看到了自己身上的不足之处，在未来还会不断地更新知识，完善本系统在各方面的设计，我们相信能够更好地满足不断变化的业务需求，并提升系统的整体性能和稳定性。在为公司创造价值的同时，也能够为客户开发出更稳定可靠的系统。