浅谈移动办公平台安全架构设计

宁　肖*
中海油信息科技有限公司信息技术分公司　天津　300452

摘　要：为了更好地解决移动办公系统与传统信息化系统的平滑对接问题，企业需深入分析移动平台办公存在的主要问题，如手机运行环境、操作方式、屏幕尺寸等，并针对这些问题进行技术创新，有效推动企业办公管理创新，加速实现企业级应用系统移动化进程，提高移动应用在企业的业务价值，为企业员工提供高效、便捷、优质的平台体验服务，同时保障企业的数据信息的安全性。

关键词：移动互联；移动平台；安全架构；安全架构

DOI：https://doi.org/10.37155/2717-5170-0305-34

1 设计思路

一般的业务应用系统核心关注点在于通过信息系统来实现某一类业务线条流程和业务过程的管理，如合同系统主要是完成从合同准备到合同归档的全生命周期管理，公文系统主要用于各类公文的线上审批流转。而移动办公平台与常规的业务应用系统截然不同，它是各类业务系统在智能终端的延伸。 这些业务系统采用的技术框架、软硬件平台、数据结构和交互模式各不相同。移动办公平台的设计思路要围绕与这些异构系统的集成展开。

考虑到移动办公平台安全的特殊性以及影响力，在移动办公平台安全架构设计中，我们需要考虑以下内容，以保证业务的连续性。

（1）完整性 ：系统的数据必须与移动办公平台生产中心的数据保持高度的一致性，该系统是对移动办公平台的完全备份。灾难发生后，原有生产中心与灾备中心之间的相互切换应尽量避免造成数据的丢失及损毁。

（2）准确性 ：系统存储的数据必须能够完全替代移动办公平台生产中心数据进行后台支撑，确保客户端数据核查的正确性。

（3）及时性：系统作为移动办公平台处理连续性的有效保证，必须确保数据的快速恢复达到恢复点要求，在最短的时间内接管并替代原生产系统，恢复正常业务处理。

（4）扩展性 ：系统建设应该提供可扩展的数据备份功能，以适应移动办公平台的不断发展。

2 架构设计

2.1 系统架构设计

移动平台架构[1]包括客户端、服务端、接口端三层，客户端需要具有基础服务，提供统一的移动应用入口与统一的应用体验，提供各类标准组件，实现各业务系统各类业务的移动操作，提供跨平台、兼容性高的移动端应用APP。服务端支撑移动门户整体功能，提供移动应用集成管理、组件管理和移动门户运营管理，并提供各类基础管理，如日志管理、安全管理、消息管理、版本管理等支撑功能，对移动接入提供配置、管理、监管服务能力，实现可视化全程监管。接口端支撑企业各类业务专业系统进行集成接入，各业务系统根据接口设计规范进行实现，更加关注业务逻辑与实现，而无需关注移动端架构设计等。

2.2 业务功能架构

移动办公平台功能建设分三个部分：终端访问、业务实现、后台综合管理。终端访问主要包含PC电脑端、安卓智能终端与苹果iOS。业务实现主要是针对第三方的业务系统，如合同、公文、BPM等业务系统的移动审批。后台管理包括设备管理、用户管理、应用管理及相关接口配置[2]。三部分功能相辅相成，完成移动办公平台数据的全过程管理。

***通讯作者：**宁肖，1989.3，女，汉，山东泰安，中海油信息科技有限公司信息技术分公司，硕士研究生， 研究方向：企业管理信息化、移动应用、软件开发与系统集成。

图1 移动办公平台技术架构逻辑图

3 安全设计

作为企业内部互联网应用的重要出口，为有效提高移动平台安全性，需对移动平台安全架构进行详细设计，满足移动办公安全需求。以移动应用需求为导向，将信息安全贯穿于数据整个生命周期，在合规性、可扩展性、传输保护等方面，统一规划移动安全设计，设计符合国家法律法规的移动应用安全方案，在功能、容量、覆盖能力等各方面，确保系统架构易于扩展，以适应业务快速变化对移动应用的要求[3]。

依托“渗透测试-查找入侵漏洞、程序修复-修复程序漏洞、应用加固-遏制问题并进行防护”三步走，从程序本身、数据通信、数据防泄漏、业务逻辑安全等多维度，提高安全性能。数据安全方面，实现应用核心数据移动端不落地、应用本地数据加密存储，如数据库、日志等、增加H5资源文件加密机制、增加文档预览水印，以及电子印章功能、增加应用防截屏功能；通信安全方面：对H5接入使用SSL加密传输；增加数据传输加密机制，实现对传输敏感数据加密、优化应用会话管理机制；业务安全方面：通过渗透测试持续优化业务应用，修复业务漏洞；通过兼容性测试持续改善业务应用运行体验；增加业务安全处理机制，包括关闭客户日志打印、会话管理等。

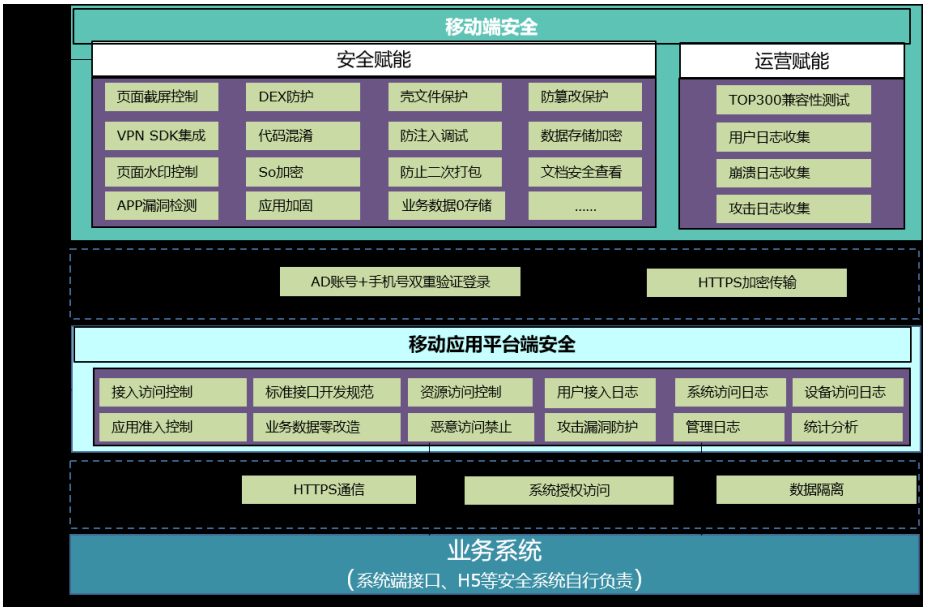

图2 移动应用安全架构图

3.1 移动端安全

移动应用需要设计有效的身份验证机制。如涉及敏感信息业务需要有二次认证机制。如果采取账号密码的认证机

制，使用强口令，口令的复杂度（包括口令组成、口令长度等）需要满足安全策略要求，且禁止传递明文口令，从而通过多重认证保证登录安全。

对于源代码层面的安全漏洞，使用专业的安全加固工具实现移动应用的自动化加固，以防护移动应用存在的风险及漏洞，实现客户端防调试、防逆向、防篡改、防劫持、防二次打包、增加设备是否root/越狱检测、增加应用安全合规策略。

对于移动应用设备，需制定设备安全监管策略，监测运行设备环境，保证运行设备安全。对用户使用设备进行记录和监管，新设备使用时需使用已有设备进行身份认证，防止用户账户密码泄漏造成的风险。

3.2 传输层安全

移动应用需要采用加密传输方式保护数据，特别是要求身份鉴别的数据内容、与外部系统交换的数据内容等。对于移动应用与内网应用互联，可以采用VPN专线连接，满足互联网访问企业内网的环境资源的问题。为确保数据的安全，客户端与VPN、内网服务器之间的各种通讯数据要进行加密处理，经过数据加密处理，有效保障数据传输过程中的安全。

3.3 访问控制

移动应用对于权限管理的设计和实现要确保服务账户或连接到外部系统的账号仅具有执行经授权的任务所需的最小权限。将许可权限尽可能地细化，使用细粒度的访问控制。移动用户每次在请求数据时提供身份凭据，移动办公平台服务器检查该身份后，再向第三方应用系统请求数据时同样也要验证核实身份凭据。该技术可保障应用系统准确获得用户身份，而确保数据不被匿名用户获取。

3.4 系统监控

除采用安全技术确保系统安全外，借助配套的软件监控系统和网络流量监控系统，通过两个监控系统对移动办公平台网络状况、操作系统、中间件、数据库的基础环境监控以及应用层监控的主要监控目标是交易成功率、交易处理状态和结果、系统队列的使用情况、通信链路、进程、线程等主要监控指标进行重点监控，同时提供可靠、迅速、精准的故障报警功能，以方便系统的维护人员能够及时分析问题、准确定位问题、迅速解决问题，第一时间发现、消除各类安全隐患，提高系统的整体安全性。

移动应用安全体系实现不能完全依赖是技术手段，同时还采取其他管理办法、制度以及审计等辅助手段来加强系统整体安全[4]。明确移动办公平台主管部门、工作岗位以及相关职责，建立移动办公平台相关管理办法、各项管理制度。且安全管理不仅在事先防范、事中管理控制，更重要的环节是事后审计，审计作为安全管理事后重要手段，审计机制对交易操作、日志等安全重点审查范围进行审计，并针对存在的安全问题进行整改和完善。

4 结束语

通过移动应用建设，对各类资源进行最大化整合，复用基础功能，减少应用竖井，规范移动应用建设，避免出现粗放式移动建设；同时通过安全架构设计，实现移动应用的有序持续发展，扩展海油移动云App长生命周期，显著提升移动应用建设效率，推动企业办公效率提升，助力数字化转型。

参考文献：

[1]于延菊.移动办公平台架构设计[J].网络安全和信息化，2020（04）：66-70.

[2]基于移动办公平台采用的关键技术研究及应用[J]. 刘延芳. 计算机产品与流通. 2019(02)

[3]关于企业移动信息安全保密方案设计的探讨 [J]. 胡兆旭 刘芳 朱尚杰 王瑾. 信息安全与技术. 2012,(10):21-22

[4]综合办公平台建设与发展的思考[J]. 陈挚. 四川农业与农机. 2020(03)