**中国医学科学院肿瘤医院**

**统一认证系统**

**技术需求**

**信息中心/计算机室**

**2018年5月**

目录

[第一部分：项目需求 3](#_Toc514139916)

[1.1. 项目概述 3](#_Toc514139917)

[1.2. 项目需求描述 3](#_Toc514139918)

[第二部分：技术需求 4](#_Toc514139919)

[2.1. 配置清单 4](#_Toc514139920)

[2.2. 产品技术要求 4](#_Toc514139921)

[第三部分：资质与服务要求 5](#_Toc514139922)

[3.1. 必要资质要求 5](#_Toc514139923)

[3.2. 非必要资质要求 6](#_Toc514139924)

[3.3. 服务要求 6](#_Toc514139925)

第一部分：项目需求

1. 项目概述

近年来，随着我院信息化的不断发展，信息系统数量不断增长，网络规模也越来越大。大量的信息系统面对大量的系统用户，各个系统的用户只能各自系统管理。这导致了工作人员需要管理不同系统的多个账号，增加了业务内容以外的不必要工作，也使得多系统协同工作的体验变差。要想解决这一问题，需要建立多系统的统一入口，其中一个关键问题就是要能对多系统、多用户做统一的管理和认证。

有了统一认证系统后，才能达到相关法规中对用户口令复杂度、密码管理等相关的要求。

1. 项目需求描述

统一认证系统应满足双因素认证机制，并且安全可靠、简单易用。用户使用时需要将获得的动态密码与静态口令同时输入，即可实现身份认证。每次使用的密码必须由算法来产生，不易破解。用户每次使用的密码都不相同，并且只能使用一次，即使黑客截获了一次密码，也无法利用这个密码来仿冒合法用户的身份。获得动态密码的形式应包括动态令牌、手机APP令牌、短信、微信发送等方式。该系统应支持以下应用：交换机、防火墙、VPN等网络设备、虚拟化设备、操作系统登录、应用软件登录、WEB应用登录等。

第二部分：技术需求

1. 配置清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **配置描述** | **数量** |
| 1 | 身份认证系统 | 支持5000个用户授权并可扩容提供认证服务，管理中心，集成动态令牌认证引擎和RADIUS服务，支持Windows和Linux操作系统，支持交换机、网络设备、应用系统、WEB登陆等等，不限制认证终端类型与应用系统数量 | 2 |

1. 产品技术要求

|  |  |
| --- | --- |
| 指标项目 | 指标要求 |
| 用户授权 | 本项目支持5000个用户授权并可扩容，不对应用系统认证数量限制 |
| 认证功能 | 提供动态口令的验证功能，接收认证代理/客户端传递的认证请求，对认证请求实施认证处理，并将处理完的结果返回给认证代理/客户端 |
| 支持动态密码认证、混合密码（动态+静态）认证、挑战/应答动态密码认证 |
| 支持SM3算法和国际标准OATH算法 |
| 采用动态多进程池机制，使系统拥有更加卓越的稳定性，提供了高并发、高性能的保障 |
| 支持主流VPN、防火墙、路由器、交换机、虚拟化等设备动态密码登录 |
| 支持Windows 2000/XP/Vista/7/8/10/Server 2003/2008/2012/2016等操作系统登录 |
| 支持Linux登录，支持Telnet、FTP、SFTP、SSH、Su登录 |
| 支持Radius认证服务 |
| 管理功能 | 提供丰富管理功能，包括操作员、应用、组域、账户、令牌生命周期、各类日志管理，并进行认证系统和安全策略的配置 |
| 采用B/S架构，易于实施 |
| 提供全面的可配置策略、参数，符合专业客户的高细腻度配置需求 |
| 全面的令牌管理、用户管理、认证终端管理、日志管理、系统管理等功能 |
| 令牌管理功能：绑定、解绑、挂失、解挂、停用、启用、解锁、同步等 |
| 支持多企业、多应用，针对应用、组、账户认证策略的管理 |
| 具备分级管理功能，可根据需求分配不同权限不同级别的管理员 |
| 用户批量导入/导出功能 |
| 支持LDAP用户，支持LDAP外部账户源认证 |
| 支持AD域用户动态密码认证 |
| 支持Windows离线认证配置管理 |
| 支持认证时间授权 |
| 支持用户自助修改静态密码 |
| 支持Radius属性值可配置 |
| 详尽的日志管理，可查询和审计令牌操作、认证过程、系统操作记录 |
| 支持SYSLOG日志服务 |
| 安全功能 | 对接入认证的应用服务器进行授权管理，未授权的服务器将无法接入认证 |
| 对身份认证软件的管理员进行授权管理 |
| 可查询系统操作及令牌操作日志 |
| 系统内所有关键数据加密存储 |
| 应用与认证服务通信加密传输 |
| 智能时间补偿技术，最大程度消除令牌失步现象 |
| 认证进程防死锁机制 |
| 高可用性 | 系统自身具备热备机制，支持第三方HA容错机制 |
| 故障告警功能，当某台服务器故障时可通知管理员 |
| 认证服务和数据库可分布式部署 |
| API接口 | 提供全面的API接口，支持Java、C/C++、PHP、ASP、JSP、.net语言接口 |
| 支持Socket和Web Service方式 |
| 提供各开发语言的接口文档、调用例程及调用演示DEMO |
| 令牌形式 | 支持硬件令牌方式 |
| 支持手机APP令牌，支持IOS和安卓 |
| 支持微信令牌，可集成至企业微信 |
| 支持短信动态密码 |
| 支持以上多种令牌形式混合使用 |
| 售后服务 | 提供3年原厂服务 |

第三部分：资质与服务要求

1. 必要资质要求
* 信息系统安全专用产品销售许可证
1. 非必要资质要求
* 软件著作权登记证书
1. 服务要求

提供三年原厂免费服务，包括软件升级，硬件质保，现场技术支持服务，永久电话支持服务。