NETCA签名验签服务器产品介绍

# 产品概述

NETCA签名验签服务器是广东省电子商务认证有限公司自主研发，一款基于PKI体系、数字签名等技术，为应用系统和用户提供数字签名、对数字签名进行有效性验证等运算服务的软硬件集成化服务器安全产品。产品内置集成硬件密码卡设备，全面支持国内标准密码算法和国际通用密码算法。NETCA签名验签服务器提供标准服务接口，应用系统通过该接口接入，保证关键业务信息的真实性、完整性和不可否认性。

NETCA签名验签服务器广泛适用于网上审批、网上招标采购、网上办公、网上支付、网上银行、医疗信息系统、网上交易等电子政务和电子商务领域中，为业务应用系统保驾护航。

# 技术标准

NETCA签名验签服务器遵循国家商用密码标准规范，主要包括。

* GM/T 0029 签名验签服务器技术规范
* GM/T 0003 SM2椭圆曲线公钥密码算法
* GM/T 0004 SM3密码杂凑算法
* GM/T 0006 密码应用标识规范
* GM/T 0010 SM2密码算法加密签名消息语法规范
* GM/T 0015 基于SM2密码算法的数字证书格式规范
* GM/T 0019 通用密码服务接口规范
* GM/T 0020 证书应用综合服务接口规范

# 产品功能

NETCA签名验签服务器符合国家商用密码相关标准规范，并且结合业务应用，提供了密钥生命周期管理、数字签名与验证签名等密码运算、用户证书管理、应用实体管理、访问权限控制等丰富的功能，其中，主要功能包括如下。

（1）密钥管理

NETCA签名验签服务器具备完善的密钥管理功能，实现对密钥整个生命周期进行统一管理与维护，保证密钥的安全。

* 密钥产生。支持产生SM2密钥对和RSA密钥对。采用符合国家密码管理局要求的商用密码卡设备，密钥采用物理噪声源产生器生成真随机数，符合随机数检测规范要求。
* 密钥存储。密钥通过加密后进行存储，保证了密钥的安全，防止密钥泄漏和非法攻击。
* 密钥备份和恢复。支持对密钥进行备份，防止操作失误、恶意删除等非常规操作导致密钥丢失，同时支持对密钥进行恢复，保证系统能够快速恢复正常使用。
* 密钥销毁。支持对密钥进行销毁。

（2）数字签名和验证签名功能

NETCA签名验签服务器支持SM2算法和RSA算法数字签名，为应用系统提供数字签名、验证签名核心功能，实现对数据、消息、文件等多种格式的运算服务。

* 数字签名：提供普通格式、PKCS#7标准的数字签名功能，SM2算法时，遵循国密相关规范格式要求。
* 验证签名：提供普通格式、PKCS#7标准的数字签名验证功能。

（3）证书有效性验证

NETCA签名验签服务器提供对证书的有效性进行验证，包括验证证书有效期、CA证书链、OCSP验证和CRL验证等多种验证方式和组合。

（4）支持多CA证书管理

NETCA签名验签服务器支持导入多CA证书或证书链进行管理，支持多CA证书验证。主要包括如下方面。

* 支持X.509 V3及PKCS系列证书的DER和PEM格式，以及国内多数CA证书机构发放的证书。
* 支持配置多个CA信任证书链，可同时导入多条CA证书链，验证不同CA的用户证书。
* 支持多个CA发布的CRL连接配置，支持动态黑名单自动更新，更新时间间隔可配置。
* 支持多个CA的OCSP连接配置，连接OCSP服务实现在线证书有效性验证。
* 提供黑名单列表证书的有效性验证，黑名单更新配置可自动定时进行。

（5）安全审计管理

NETCA签名验签服务器提供全面的安全日志记录功能，日志记录、查看、审计和导出功能。审计日志包括：管理员操作行为日志、异常信息日志、对接应用接口的调用审计日志。确保签名验签服务器安全可靠，行为可审计、可追溯。

（6）系统管理

NETCA签名验签服务器提供了对系统进行维护和管理的功能，便于系统管理员进行日常维护。支持NTP时间源同步，实现定时同步时间；系统信息配置；服务器证书安装；查看系统运行状态；网络配置等功能，为管理员提供便捷操作，满足日常维护需要。

（7）用户证书管理

NETCA签名验签服务器提供了对用户证书进行管理，包括用户证书的导入导出、存储、验证、冻结与激活以及过期证书查询等，对用户证书进行统一管理和维护，同时也提供了多种证书验证策略进行配置，实现对用户证书不同的验证方式。

（8）访问权限控制

NETCA签名验签服务器采用强身份认证机制实现访问控制，系统分为管理员和审计员两种角色管理，管理员负责系统相关配置，审计员负责日志管理。系统为每一个管理员和审计员颁发数字证书，通过电子密匙数字证书方式登录，在进行核心操作时需要进行数字签名，并保存在系统中用于日志审计。

（9）应用开发接口

NETCA签名验签服务器遵循GM/T 0029 签名验签服务器技术规范的消息协议要求，提供强大的接口，包括导出证书、解析证书，解析获取证书信息、验证证书有效性、数字签名与验证、消息签名与验证。支持多种开发语言下使用接口接入，实现签名验签应用。

# 产品性能

暂无。

# 运行环境

表5-1 NETCA签名验签服务器运行环境

|  |  |
| --- | --- |
| **操作系统** | Linux操作系统，如：CentOS 7.5 |
| **支持环境JDK** | JDK8 |
| **WEB服务** | Tomcat9 |
| **数据库系统** | MySQL 5.7或以上 |
| **NETCA安全中间件** | NETCA安全中间件V5.0或以上 |

# 产品优势

NETCA签名验签服务器遵循国家商用密码相关标准规范，提供了强大的应用开发接口，适用于各种开发应用需求，同时保证了提供安全高可靠性的访问服务。

（1）符合标准规范

NETCA签名验签服务器遵循GM/T 0029《签名验签服务器技术规范》、GM/T 0015 《基于SM2密码算法的数字证书格式规范》、GM/T 0010《SM2密码算法加密签名消息语法规范》、GM/T 0004《SM3密码杂凑算法》、GM/T 0019《通用密码服务接口规范》等国家商用密码标准规范，保证系统的通用性和标准性。

（2）安全性

* 全面支持SM1、SM2、SM3、SM4国家标准密码算法以及支持SHA1、SHA-256、SHA-384、SHA-512、RSA等国际通用密码算法。
* NETCA签名验签服务器使用符合国家密码管理局要求具有商用密码资质的密码卡硬件设备，具有防读取、防篡改等抗攻击特性，能够保证密码算法使用过程中的安全性。
* NETCA签名验签服务器所使用的业务应用系统证书、用户证书、系统用户证书由NETCA第三方权威CA颁发机构签发，确保证书的合法性、有效性。
* NETCA签名验签服务器支持SSL/TLS协议，保证通信过程数据保密性，同时系统操作过程使用电子密匙数字证书强身份认证方式，保证系统安全，防止非法入侵。

（3）高性能密码运算

NETCA签名验签服务器提供SM2与RSA数字签名与验证、消息签名与验证功能，采用了国家密码管理局批准使用的高速公钥密码算法芯片，提高了运算速度和信息的安全性。提供高质量随机数，密钥的产生采用物理噪声源产生器生成真随机数，符合随机数检测规范要求。

（4）易用性

NETCA签名验签服务器提供友好便捷的用户操作界面，管理员和审计员可以通过Web方式对系统进行管理和维护。

（5）完备的应用开发接口

NETCA签名验签服务器提供导出证书、解析证书，解析获取证书信息、验证证书有效性、数字签名与验证、消息签名与验证。支持多种开发语言下使用接口接入，与业务应用系统解耦，实现签名与验证应用。

（6）可靠性

NETCA签名验签服务器采用可靠性强的硬件服务器，可实现负载均衡和冗余备份/数据备份，支持双机热备，具有高可靠性。NETCA签名验签服务器采用密码卡设备对数据进行签名，确保签名过程安全可靠。

# 产品资质

暂无。

# 应用案例

1）广东省信息中心项目

2）广西医科大第一附属医院项目

3）珠海子CA项目

# 附录

## 产品文档清单

* <http://192.168.0.11:8081/svn/rdrelease/软件发布/签名验签服务器/8.发布说明/NETCA签名验签服务器用户手册.doc>
* <http://192.168.0.11:8081/svn/rdrelease/软件发布/签名验签服务器/8.发布说明/NETCA签名验签服务器介绍.pptx>