**网证通安全中间件白皮书**

目录

[一、产品简介 3](#_Toc457805898)

[二、产品特点 3](#_Toc457805899)

[2.1应用环境 3](#_Toc457805900)

[2.2 API接口 3](#_Toc457805901)

[2.2 支持算法 3](#_Toc457805902)

[三、产品功能 4](#_Toc457805903)

[3.1 加密运算 4](#_Toc457805904)

[3.2 证书及其管理 4](#_Toc457805905)

[3.3 数字信封 5](#_Toc457805906)

[3.4 SignedData 5](#_Toc457805907)

[3.5 时间戳 5](#_Toc457805908)

[3.6 S/MIME 6](#_Toc457805909)

[3.7 XML签名 6](#_Toc457805910)

[四、产品优势 6](#_Toc457805911)

[4.1 安全性 6](#_Toc457805912)

[4.2 易用性 6](#_Toc457805913)

[4.3 规范化 7](#_Toc457805914)

[4.5 通用性 7](#_Toc457805915)

[4.6 跨平台 7](#_Toc457805916)

[4.7 可扩展性 8](#_Toc457805917)

# 一、产品简介

网证通安全中间件（以下简称：NETCA CRYPTO）是广东省电子商务认证有限公司独立自主研发的产品。NETCA CRYPTO是一个PKI开发库，主要包括基本的加密算法、证书及其管理、数字信封、SignedData、时间戳、S/MIME和XML签名等功能。

NETCA CRYPTO支持RSA证书和SM2证书的相关操作。目前，国产算法SM2是国家主推的非对称运算算法，但第三方应用很难甚至不能兼容SM2算法。NETCA CRYPTO不仅全面支持国产算法，而且兼容第三方应用。其中，CNG接口实现了一个加密提供者，在Windows系统中使用，利用CryptoAPI来使用SM2的证书；支持SM2证书在PDF文件上的签名以及验签。NETCA CRYPTO 提供了JCE扩展包，支持使用RSA和SM2证书进行签名和验证。

# 二、产品特点

## 2.1应用环境

Windows：支持Windows 2000及其以上的操作系统，包括32位和64位。

Linux：支持RedHat企业版5、6和7，包括32位和64。

## 2.2 API接口

支持多种主流开发语言，NETCA\_CRYPTO提供了JAVA接口、COM接口、.NET、C/C++接口、CSP接口、CNG接口、JCE接口。

## 2.2 支持算法

* **Hash**

SHA-1、SHA-256、SHA-384、SHA-512、SM3等。

* **Mac**

HMAC-SHA1、HMAC-SHA256、HMAC-SHA384、HMAC-SHA512、 HMAC-SM3、AES-CMAC等。

* **对称加密**

AES、SM4、SSF33、SM1等。其中，SSF33和SM1需要加密硬件的支持。

* **非对称加密**

PKCS#1 V1.5 RSA加密、SM2加密。

* **密钥协商**

ECDH、SM2。

* **数字签名**

SHA1WithRSA、SHA256WithRSA、SHA512WithRSA、ECDSAWithSHA1、ECDSAWithSHA256、ECDSAWithSHA512、SM3WithSM2。

# 三、产品功能

## 3.1 加密运算

* 支持Hash运算。
* 支持Mac运算。
* 支持对称加解密运算。
* 支持非对称加解密运算。
* 支持密钥协商。
* 支持数字签名。

## 3.2 证书及其管理

证书通常指X.509证书。NETCA CRYPTO提供了证书解析、证书验证、签名以及解密等功能。

* 证书解析：解析证书版本、证书主体、公钥编码、公钥算法、密钥用途、颁发者、有效期等信息以及扩展项。
* 证书验证：提供验证有效期、验证证书链、验证CRL、验证OCSP方法。
* 证书操作：提供签名、验证签名、加密和解密的方法。
* 证书管理：提供个人证书库、联系人证书库、CA证书库和根证书库等相关操作。

## 3.3 数字信封

* 提供了构造数字信封以及数字信封解密的方法。
* 支持IETF STD70的EnvelopedData。可以支持密钥传输和密钥协商方式。
* 支持国密GM/T 0010-2012的EnvelopedData。

支持颁发者名和证书序列号的组合或者主体密钥标识符来标识接收者的身份。

支持一个或者多个接受者。

* 支持大数据的处理。

## 3.4 SignedData

提供了SignedData签名以及验证的方法。

支持IETF STD70的SignedData。

国密GM/T 0010-2012的SignedData。

支持带原文和不带原文的两种签名方式。

支持颁发者名和证书序列号的组合或者主体密钥标识符来标识接收者的身份。

支持多人签名和联署签名。多人签名是多个人对同一数据的签名，联署签名是对签名值的签名。

支持多种CadES（CMS Advanced Electronic Signatures）。包括CAdES-T、CAdES-C、CAdES-X Long、CAdES-X Type1、CAdES-X Type2等。

## 3.5 时间戳

* 支持RFC3161时间戳。
* 提供时间戳签名以及时间戳验证的方法。

## 3.6 S/MIME

* S/MIME是在MIME上面应用一些安全特性，主要包括SignedData和数字信封，保证邮件主体的安全。

## 3.7 XML签名

* 支持W3C的标准
* 支持签名者绑定，签名策略，长期签名等功能。

# 四、产品优势

## 4.1 安全性

* 算法安全。

1. 全面支持国产密码算法SM1、SM2、SM3、SM4、SSF33。
2. 支持通用密码算法3DES、AES、RSA、SHA256、SHA384、ECC 等。

* 密钥安全。

1. 采用通过国密局审批的硬件密码设备，包括usbkey、IC卡、加密卡、加密机，产生、存放密钥对（公钥和私钥）。
2. 私钥的运算在密码设备运算，不以任何明文的方式出现在设备之外。
3. 通过口令方式控制私钥的访问权限。

## 4.2 易用性

加密运算一般要求开发人员具有较强的PKI专业知识。为了尽可能降低对开发人员的专业知识要求，NETCA CRYPTO提供了：

* 通俗易懂的开发接口，支持多种主流开发语言。
* 逻辑清晰、操作简单的步骤。

## 4.3 规范化

NETCA CRYPTO是遵循国际标准和国密标准。

* GM/T 0003 SM2椭圆曲线公钥密码算法
* GM/T 0002 SM4分组密码算法
* GM/T 0004 SM3密码杂凑算法
* GM/T 0009 SM2密码算法使用规范
* 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
* RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
* RFC 2633 S/MIME Version 3 Message Specification
* RFC 3275 XML-Signature Syntax and Processing
* RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
* RFC 5816 ESSCertIDv2 Update for RFC 3161
* RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
* RFC 5652 Cryptographic Message Syntax (CMS)

## 4.5 通用性

* 支持微软office文档签名和adobe PDF签名。其中，PDF签名支持RSA和SM2证书。
* 支持IE、Chrome浏览器。

## 4.6 跨平台

* 支持主流的操作系统windows、linux。

## 4.7 可扩展性

* 兼容多款密码设备。

目前，已经支持飞天诚信、海泰方圆、文鼎创、山东得安、江南天安等多个厂家的密码设备。如果应用需要其他厂家的密码设备，不用改变或者调整上层的应用程序，可以做到无缝的接入。