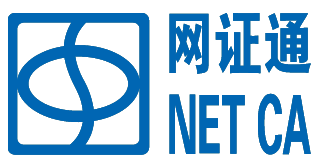
密级：限制

编号：NETCA-T01-PR03-RE04



微信小程序平台中间件

需求说明书

（V1.0版）

文件控制信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 文件名 | 微信小程序平台中间件需求说明书 | | 受控状态 | √是 □ 否 |
| 编号 | NETCA-T01-PR03-RE04 | | 版本号 | V1.0 |
| 密级 | □核心商密 □普通商密 √限制 □公开 | | 保密期限 | 长期 |
| 起草人 |  | 批 准 人 |  | |
| 批准日期 | 2020年 06 月XX 日 | | | |
| 生效日期 | XXXX年 XX 月XX 日 | | | |

密级说明：

1. 核心商密：是指企业最重要的商业秘密，泄漏后会使企业利益遭受特别严重的损害；
2. 普通商密：是指企业重要的商业秘密，泄露后会使企业利益遭受比较严重的损害；
3. 限制：是指仅在企业范围内使用，不对外公开的商业秘密，泄露后可能会使企业利益遭受损害；
4. 公开：是指可向公司以外人员随意公开的非商业秘密。

文件版权说明

（1）本文件是广东省电子商务认证有限公司的内部管理文件，其版权归广东省电子商务认证有限公司所有，版权内容包括文件格式及内容。

（2）任何人或组织未经广东省电子商务认证有限公司授权，不得对本文件进行复制、传播，更不得用于商业用途。

|  |  |
| --- | --- |
| 版 本 | 说 明 |
| V1.0 | 初始版本 |
| V2.0 | XXXX |
| V2.1 | XXXX |

目 录

[1 引言 1](#_Toc44494767)

[1.1 目的 1](#_Toc44494768)

[1.2 背景 1](#_Toc44494769)

[1.3 参考资料 1](#_Toc44494770)

[1.4 术语 1](#_Toc44494771)

[2 任务概述 2](#_Toc44494772)

[2.1 目标 2](#_Toc44494773)

[2.2 系统（或用户）的特点 2](#_Toc44494774)

[3 假定和约束 2](#_Toc44494775)

[4 需求总体说明 2](#_Toc44494776)

[4.1 软件功能说明 2](#_Toc44494777)

[4.2 对功能的一般性规定 5](#_Toc44494778)

[4.3 对性能的一般性规定 6](#_Toc44494779)

[4.4 对安全性的要求 6](#_Toc44494780)

[4.5 其他专门要求 6](#_Toc44494781)

[5 运行环境规定 6](#_Toc44494782)

[5.1 设备及分布 6](#_Toc44494783)

[5.2 支撑软件 6](#_Toc44494784)

[5.3 接口 6](#_Toc44494785)

[6 版本规划 7](#_Toc44494786)

[6.1 版本1 7](#_Toc44494787)

[6.2 版本2 7](#_Toc44494788)

[6.3 版本3 8](#_Toc44494789)

[6.4 版本4 8](#_Toc44494790)

[7 附录 8](#_Toc44494791)

[附录一 8](#_Toc44494792)

[附录二 9](#_Toc44494793)

[附录三 11](#_Toc44494794)

**微信小程序平台NETCA Crypto中间件需求说明书**

# 引言

## 目的

指导开发者和测试者按照需求提出的功能进行开发和测试。

## 背景

目前公司在Windows、Linux、Android、IOS等平台上具有功能完善的中间件，但尚没有微信小程序平台（下文所涉及的小程序在没有特别指出时均是指微信小程序）上可供使用的中间件。随着项目需求的扩展，出现了在小程序平台上使用数字证书进行签名、加解密等的应用，为了满足小程序平台上应用的需求，特准备开发小程序平台上的中间件。

## 参考资料

1. NETCA PKI 中间件其它语言或平台系列文档
2. 微信小程序开发平台， <https://mp.weixin.qq.com/cgi-bin/wx?token=&lang=zh_CN>

## 术语

中间件：在没有特别明确指明的情况下，本文档中所描述的中间件均是指NETCA Crypto 中间件。

NETCA Crypto中间件插件: 一个符合微信小程序平台的插件，本需求文档所描述的任务目标之一，由NETCA研发和发布，其它小程序直接集成NETCA Crypto中间件插件的基础功能。

# 任务概述

## 目标

**NETCA Crypto 中间件插件**

本次研发活动的目标是开发出一个符合微信小程序平台规范要求的小程序插件，该小程序插件命名为“NETCA Crypto中间件”，其可以被第三方小程序直接集成调用。

“NETCA Crypto 中间件”插件对外提供的功能类似于NETCA CRYPTO PC版的基础功能，具体功能见下文。

## 系统（或用户）的特点

NETCA Crypto 中间件插件的用户是第三方小程序开发者，具备集成微信小程序插件的基本能力，但第三方开发者不一定深入了解PKI方面的知识，因此，NETCA Crypto小程序和SDK包应提供一部分粗粒度的接口封装，把部分细节进行隐藏。

# 假定和约束

1. 开发流程和使用的技术需要遵循微信小程序平台和支付宝小程序平台的规范。
2. 微信小程序平台下的代码在不需要大量调整的基础下可以转换到支付宝小程序平台上。

# 需求总体说明

## 软件功能说明

### 密钥对管理

1、支持两种类型的密钥对：一种是利用密钥分割原理实现的移动Key的密钥对，当前这种密钥对仅支持SM2算法。另外一种是本地存储的完整的密钥对，要求进行加密存储，而且仅当前小程序可以访问，这种密钥对可以支持RSA算法和SM2算法。

2、使用密钥对需要验证用户口令。

3、如果实现支持，考虑解锁口令。

### 证书管理

#### 申请证书

1. 支持由第三方审核，CA只负责签发证书的模式。
2. 支持由第三方提交资料，CA负责审核，签发等工作的模式。
3. 支持由CA录入资料，CA审核，签发等工作的模式。

详细说明见章节 4.1.10[申请证书](#_申请证书)。

#### 续期证书

1、支持对证书进行续期，操作流程可参考USBKey证书续期。

#### 产生证书请求

1. 支持PKCS#10的证书请求的生成。
2. 支持SM2，RSA算法。

#### 验证证书

1、支持根据配置的根证书和CA证书来构造证书路径并进行验证。初始版本可以仅支持最简单的验证，不包括名字约束、策略等。

2、支持使用CRL来验证证书的状态。CRL仅要求支持最基本的完整CRL。

3、支持使用OCSP来验证证书的状态。OCSP要求支持三种信任模式。

4、支持根据AIA的CA版本者地址来获取CA证书

5、支持根据CRL DP中的地址获取CRL

6、支持根据AIA的OCSP地址来访问OCSP

#### 证书解析

1、支持获取证书的颁发者名、主体名、有效期、序列号、公钥等基本信息

2、能够区分证书是RSA证书还是SM2证书

3、能够根据密钥用法区分证书是签名证书还是加密证书

4、支持获取字符串编码的扩展值，以及NETCA常用的扩展值

### 产生随机数

1. 支持移动Key协作系统方式的获取随机数
2. 如果可以的话，支持完全从本机获取足够的熵来产生随机数
3. 产生的随机数应通过扑克测试才能使用

### P1签名/验签

1、签名和验证签名支持SM3WithSM2和Sha256WithRSA

### 加密/解密

1. 对称加解密支持SM4和AES
2. 非对称加解密支持SM2和RSA

### SignedData

1. 支持带原文和不带原文的SignedData的签名和验证，仅要求支持单个签名。初始版本仅要求支持本身带证书的SignedData的验证。
2. 支持产生DER编码的SignedData和验证DER编码的SignedData
3. 支持验证BER编码的SignedData
4. 既支持SignedData带签名属性也支持不带签名属性
5. SM2的SignedData支持GB/T 35275-2017的格式，也可以支持RFC 5652的格式。RSA的SignedData支持RFC 5652的格式
6. 支持CAdES-E-BES格式，也就是支持content-type、message-digest、signing-certificate、signing-certificate-v2签名属性
7. 支持CAdES-E-T格式，也就是在CAdES-E-BES格式的基础上增加支持signature-time-stamp不签名属性。
8. 支持使用颁发者名和序列号标识签名者，也可以支持主体密钥标识符标识签名者。

### 数字信封

1. 支持密钥传输方式的数字信封EnvelopedData，也就是直接使用证书加密对称密钥的方式。
2. SM2的EnvelopedData支持GB/T 35275-2017的格式，也可以支持RFC 5652的格式。RSA的EnvelopedData支持RFC 5652的格式
3. 支持使用多个证书的数字信封
4. 对称加密算法支持SM4-CBC和AES128-CBC。必须支持SM2和SM4的组合，RSA和AES的组合，其他组合方式不要求。

### 电子签章

支持PDF电子签章，包括定点签章，关键字签章。

支持电子印章的读写。

### 算法支持

* 签名：SM3WithSM2、Sha1WithRSA, Sha256WithRSA, Sha512WithRSA
* 对称加解密: SM4\_ECB, SM4\_CBC、AES\_ECB, AES\_CBC
* 非对称加解密:SM2、RSA
* Hash: SM3、Sha1, Sha256, Sha512
* HMAC: HMAC-SM3、HMAC-SHA1, HMAC-SHA256, HMAC-SHA512

### 申请证书

NETCA Crypto中间件支持以下两种途径审核用户身份：

* 由第三方审核用户身份
* 由网证通审核用户身份

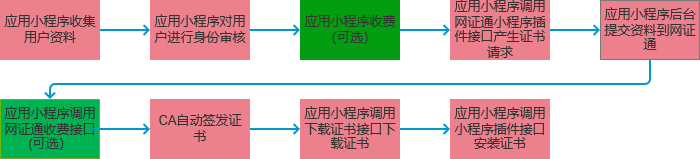
#### 第三方审核用户身份

当采用第三方审核用户身份时，网证通完全信任第三方审核的数据，第三方将审核后的用户数据提前发送到网证通业务平台。

网证通和第三方之间需通过相应的协议约束用户身份审核的真实性。

第三方业务系统在把数据推送到网证通业务平台时，必须对数据进行签名保护。

第三方审核用户时，申请证书的流程如下：



#### 网证通审核用户身份

##### 申请自然人证书

###### 身份验证方式

网证通审核自然人身份的途径主要包括以下方式：

* 短信验证

通过短信校验码验证自然人是否持有输入的手机号码的手机，验证过程中不会去验证手机号码是否归属于自然人名下。

* 拍摄身份证图片上传校验

此验证过程要求用户拍摄合法有效的身份证正反面，并上传拍摄后的身份证图片。使用拍摄而非从相册中选择的目的是证明用户拥有实体身份证。

* 刷脸认证（活体检测+身份证权威数据比对）

通过刷脸操作，确认当前操作者是否和输入的姓名，身份证信息标识的是同一个人。刷脸认证过程中包含活体检测，权威数据比对。

* 组合验证

将以上几种验证方式组合起来验证用户身份。可用的组合方式包括：

1. 短信验证 +  拍摄身份证图片上传校验 + 刷脸认证
2. 短信验证 + 刷脸认证
3. 短信验证 + 拍摄身份证图片上传校验
4. 拍摄身份证图片上传校验 + 刷脸认证

###### 申请流程

应用系统提前推送用户资料

第三方系统提前把用户数据推送给网证通业务平台，则NETCA Crypto 中间件提供的小程序插件申请证书过程中就不需要再次收集用户资料信息，整个申请证书的过程主要是验证用户身份，验证身份的途径依据项目的需求进行配置，NETCA Crypto中间件小程序插件的主要业务流程如下：

1. 展示协议内容，并要求用户勾选同意协议后才能进行下一步。
2. 如果该项目配置了要进行短信验证，则通过短信验证手机号，如果手机号是接口传入，不允许用户修改，验证通过后进行下一步。如果该项目没有配置进行短信验证，则需要应用系统提供一个签名授权，保证用户身份已经经过验证。
3. 利用手机号等参数信息查询用户信息，如果用户信息不存在，则提示用户信息尚未上传，等待系统上传用户信息。
4. 展示用户信息。
5. 如果该项目配置了“拍摄身份证图片上传校验”验证且用户尚未上传身份证正反面图片，则跳转到身份上传界面。上传身份证图片的过程中，要比对上传的图片和应用系统推送过来的用户资料中的身份证号，姓名等信息是否匹配。
6. 如果该项目配置了“刷脸认证”，且尚未经过刷脸认证，则进入刷脸认证流程。
7. 如果该项目配置了收费，且用户尚未缴费，则进入缴费流程。
8. 如果用户完成了以上步骤，则产生证书请求，提交证书申请。
9. CA自动审核，签发证书。
10. NETCA Crypto中间件小程序插件安装证书。

用户手动录入资料

如果第三方业务系统没有把用户数据推送给网证通业务平台，需要NETCA Crypto中间件自己收集用户资料，完成身份审核。NETCA Crypto中间件小程序插件的主要业务流程如下：

1. 展示协议内容，并要求用户勾选同意协议后才能进行下一步。
2. 如果该项目配置了要进行短信验证，则通过短信验证手机号。手机号码如果是通过接口传入，不允许用户修改，验证通过后进行下一步。如果该项目没有配置进行短信验证，则需要应用系统提供一个签名授权，保证用户身份已经经过验证。
3. 利用手机号等参数信息查询用户信息，如果用户信息不存在，则跳转到步骤5，如果信息已经存在，则进行步骤4。
4. 展示用户信息，执行步骤8。
5. 如果该项目配置了“拍摄身份证图片上传校验”验证，则跳转到身份证上传界面。
6. 如果执行了步骤4，则展示手机号码，上传身份证OCR的结果信息（姓名，证件类型，身份证号）且这些信息不允许修改，用户选择证书有效期（如果项目模板允许选择）。
7. 如果没有执行步骤4，则允许用户手动输入姓名，身份证号码，选择证书有效期（如果项目模板允许选择）。
8. 如果该项目配置了“刷脸认证”，且尚未经过刷脸认证，则进入刷脸认证流程。
9. 如果该项目配置了收费，且用户尚未缴费，则进入缴费流程。
10. 如果用户完成了以上步骤，则产生证书请求，提交证书申请。
11. CA自动审核，签发证书。
12. NETCA Crypto中间件小程序插件安装证书。

## 对功能的一般性规定

小程序风格遵循小程序平台要求。

## 对性能的一般性规定

无

## 对安全性的要求

## 其他专门要求

视具体情况，列出不在本规范规定中的需求，如对数据库的要求，多平台特性要求，操作特性要求，场合适应性要求等对一具体软件系统的所有功能（或一部分）的共同要求，针对某一功能的专门要求应列在该功能说明中。

# 运行环境规定

## 设备及分布

1） Android，IOS 手机

## 支撑软件

1. 微信小程序平台
2. 支付宝小程序平台

## 接口

无。

# 版本规划

## 版本1

版本1是初始版本，包括：NETCA Crypto SDK（小程序版）。主要支持利用密钥分割原理实现的移动Key的密钥对，支持SM2算法，产生证书请求，安装证书，证书解析获取基本信息，证书验证，SignedData等功能

具体如下：

算法支持主要是国密的算法，包括SM2签名和SM3 Hash

密钥对的支持利用密钥分割原理实现的移动Key的密钥对

具体功能如下：

4.1.1[1]的利用密钥分割原理实现的移动Key的密钥对。4.1.1[2]

4.1.2.1[2]和4.1.2.3[1]。这两个能保证安装签名证书，有了证书SignedData才能实现

4.1.2.4[1]和[2]。这个是最基本的证书验证。（如果要求OCSP优先把[2]替代为[3]）

4.1.2.5[1]、[2]、[3]、[4]

4.1.3[1]

4.1.4[1]仅要求支持SM3WithSM2

4.1.6[1]、[2]、[4]、[5]中至少支持GB/T 35275-2017的格式

## 版本2

版本2主要在版本1的基本上增加本地存储的完整的密钥对的支持和RSA算法的支持。同时完整的证书验证和带时间戳的SignedData。

具体新增如下：

算法新增支持主要是RSA相关的算法，包括RSA签名和SHA-2和SHA-1 Hash

密钥对新增支持本地存储的完整的密钥对

具体新增功能如下：

4.1.1[1]的本地存储的完整的密钥对。

4.1.2.4[3]、[4]、[5]、[6]

4.1.4[1]新增支持Sha256WithRSA

4.1.6[5]要求SM2同时支持GB/T 35275-2017的格式和RFC 5652的格式，RSA支持RFC 5652的格式、[6]、[7]。

## 版本3

版本3主要是增加NETCA Crypto 小程序，融入证书申请流程。

具体新增功能如下：

4.2.2.1[1]

4.2.2.2[1]

## 版本4

版本4主要是增加加密和数字信封相关功能。

具体新增如下：

算法新增支持主要是SM2加密和RSA加密，SM4加密和AES加密

具体新增功能如下：

4.1.5[1]和[2]

4.1.7[1]、[2]、[3]、[4]

# 附录

## 附录一

需求分析过程中会产生各种记录如调查表格、业务系统单据等。记录或报告的存档编号和名称填写在下表中。其中类别是记录的分类，一般有业务系统说明书、业务系统数据说明书、业务系统调查表、原始数据单据、业务系统参考资料。

|  |  |  |
| --- | --- | --- |
| 编号 | 名称 | 类别 |
|  |  |  |
|  |  |  |

## 附录二

需求分析报告评审记录

记录编号： 时间： 年 月 日

|  |  |  |
| --- | --- | --- |
| 项目编号： | 项目名称： | |
| 项目软件经理PSM： | 需求分析报告编制人： | |
| 参加评审人员： | | |
| 评审内容：(评审中审议通过的内容在“□”中划“√”，否则划“×”)  1. 无岐义性 □  2. 完整性 □  3. 可验证性 □  4. 一致性 □  5. 可使用性 □  6. 符合《需求分析报告编写规范》的要求 □ | | |
| 评审意见： | | |
| 风险评估总结： | | |
| 评审结论：(评审中审议通过的内容在“□”中划“√”，否则划“×”)  1. 通过评审，可以进入下一阶段 □  2. 未通过评审，修改后重新评审 □ | | |
| 填表： | | 审批： |

1. 本页不足记录结果时，可以有附页，附页格式自定。总页数包括本页与所有附页。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 附录三 **风险评估与控制（需求分析报告评审附页）** | | | | | |
| 系统设计报告名称： | | 报告编号： | | | 评审部门： |
| 序号 | 风险描述 | 风险发生可能性 | 风险级别 | 风险现值 | 风险控制措施 |
| 1 | 客户需求变化 |  |  |  |  |
| 2 | 开发人员缺乏足够的行业知识和专业知识 |  |  |  |  |
| 3 | 需求未被顾客完全认可 |  |  |  |  |
| 4 | 需求不明确 |  |  |  |  |
| 5 | 时间紧 |  |  |  |  |
| 6 | 存在技术问题、采用新技术 |  |  |  |  |
| 7 | 多部门配合 |  |  |  |  |
| 8 | 没有顾客系统接口原型 |  |  |  |  |
| 9 | 缺乏顾客自然情况的了解 |  |  |  |  |
| 10 | 顾客配合程度不够 |  |  |  |  |
| 11 |  |  |  |  |  |
| 1. 评估中风险不限于表中已列出的，应依据评审的具体情况增加风险项。并将各项填写完整。 2. 风险描述：描述当前过程中可能发生的风险。风险发生可能性：风险发生的概率，以百分数表示，为0到1，增量为0.05。风险级别：风险发生造成损失的严重程度，以0~10级-示，其中10级 为最高级。风险现值：风险发生可能性与风险级别的乘积。风险控制措施：预防风险发生的措施。 | | | | | |