用友 NC6.X-CFCA 集成

需求分析报告

（版本：**1.0** ）

中国金融认证中心

2015 年 04 月 01 日

修订记录

序号	版本	修改日期	修改内容	修订人	修订人
1	1.0	2015-04-01	创建文档，描述需求	马奔	张庆安

目录

TOC \o "1-3" \h \z \u 1 概述 4

1.1 项目描述 4

1.2 运行环境 4

1.2.1 硬件环境 4

1.2.2 软件环境 4

1.3 条件与限制 5

2 需求规定 5

2.1 功能需求 5

2.1.1 系统结构 5

2.1.2 功能描述 6

2.2 性能需求 9

2.2.1 兼容性 9

2.2.2 稳定性 9

2.3 运行需求 10

2.3.1 外部接口 10

概述

1. 项目描述

用友 NC6.X 系统与 CFCA 进行集成，只实现校验的部分。由用友方提供接口定义，CFCA 进行实现。校验过程中需要从 RA 服务器获取证书，需要连接 RA 服务器。

1. 运行环境

1.1. 硬件环境

产品	最低配置
NC 6x 系统	请参考 NC 6x 系统的需求
RA Server	需要能够连接 RA 服务器

1.1. 软件环境

1.1.1. 服务器端

支持 Windows7、Linux。

1.1.1. 第三方产品

1.1.1.1. RA 服务器

本接口需要从 RA 服务器调用证书、确认证书状态，需要连接用友自建的 RA 服务器。

1. 条件与限制

运行产品需要有JAVA运行环境，且版本是1.6及其以上版本。

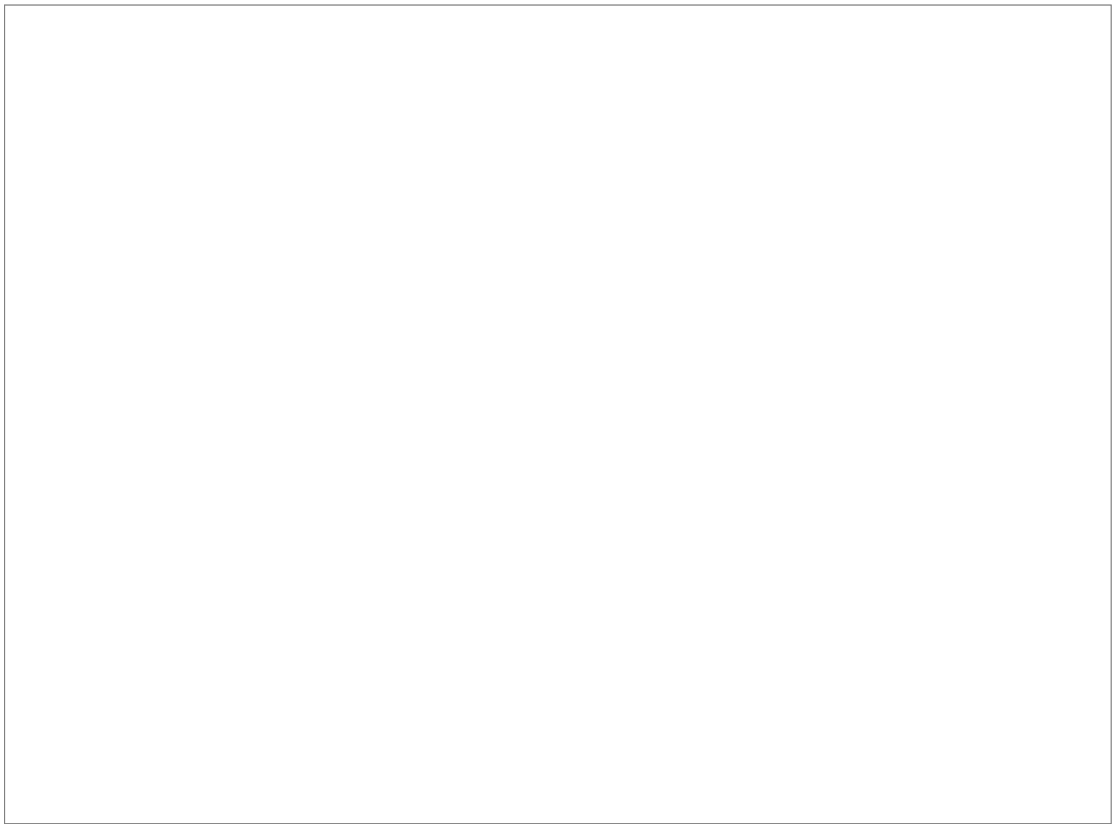
需求规定

1. **功能需求**

1.1. **系统结构**

由用友方提供接口定义，CFCA进行实现。用友将证书的序列号、原文、签名值传入，校验类根据序列号从RA服务器获取对应的证书，如果证书是激活状态，使用该证书进行校验，返回用友在ISecurityConstant类中定义的返回值。

使用时需要将校验类在ierp\sf\caRegisterCenter.xml配置文件中进行注册，校验过程中需要从RA服务器获取证书，需要连接RA服务器。



1.1. **功能描述**

1.1.1. **校验实现**

1.1.1.1. **用友接口实现**

由用友方提供接口定义，CFCA负责实现校验部分。

CFCA需要实现接口，并通过xml文件进行注册，用友调用实现的接口进行校验。

本接口的实现调用了 RA 服务器，根据用友传入的证书序列号从 RA 获取证书，并判断证书的状态，如果证书是激活可用状态，使用该证书对用友传入的原文和签名值进行校验，返回校验结果。

用友接口定义如下：

```
* 验证签名

*

* @param certSN

* 证书的序列号

* @param plainText

* 原文

* @param signatrue

* 签名值

* @return 签名结果，如果验证成功，返回 ISecurityConstant.SIGNATURE_VALID.

* @throws Exception

* @see 更多的返回值参见{@link ISecurityConstant}

*/

public int verify(String certSN, byte[] plainText, byte[] signatrue) throws Exception;

/**

* 对一个 xml 格式的字符串进行验证，

*

* @param certSN

* 证书的序列号

* @param xmlPlainStr

* 业务对象的 xml 描述的字符串

* @param singature

* {@link ISigner#signWithXML(String)}签名的返回值

* @return

* @throws Exception

*/
```

public int verifyWithXML(String certSN, String xmlPlainStr, byte[] signatrue) throws Exception;

1.1.1.1. 接口返回值

返回值	含义
ISecurityConsts.SIGNATURE_INVALID (201)	校验成功
ISecurityConsts.SIGNATURE_INVALID (204)	校验失败，比如原文错误的情况
ISecurityConsts.CERTIFICATE_NOT_IN_VALID_PERIOD (207)	证书不在有效期，比如证书已经过期的情况
ISecurityConsts.DOWNLOAD_CRLFILE_ERROR (214)	下载证书错误，比如不存在的证书序列号，RA 接口会返回空，这种情况给用友返回证书下载失败
ISecurityConsts.CERTIFICATE_PARSE_ERROR (210)	证书解析失败，目前的 RA 服务器返回的公钥是用 base64 编码的，接口获取公钥之后用 base64 解码，如果解码失败，返回解析错误
ISecurityConsts.VERIFICATION_EXCEPTION (304)	校验异常，比如配置文件中写了不支持的算法一类错误，任何在校验中可能发生的错误都返回这个值

1.1.1.1. 配置文件

系统的常量参数写在配置文件中，包括 RA 服务器的连接等配置需要设置好，配置文件会在第一次调用读取类的时候进行加载并缓存。

RA 服务器的连接支持 http 和https 两种方式，具体请见 config/app.properties 配置文件的如下两个配置：

```
#ra 连接类型 1-http ,2-https

ra.type=2

#ra 连接地址，http 和https 两种方式

ra.http.url=https://192.168.93.96:3443/RA/CSHttpServlet
```

1.1.1.1. 证书缓存

为了提高性能，使用了缓存，缓存使用 hashMap 进行实现，提供定时刷新功能和缓存上限控制，具体请见 config/app.properties 配置文件的如下两个配置：

```
#缓存的个数，小于等于零不限制
```

cache.size=10000

#缓存失效时长，毫秒，小于等于零不失效，86400000=一天

cache.duration=86400000

1. 性能需求

优先级：A1 优先级最高，它是必须要实现的功能；A2 优先级次高，它是将来可能要实现的功能，依次类推。

1.1. 兼容性

级别	内容	备注
A1	支持 Windows7、Linux	1 需要 jdk1.6 及以上

1.1. 稳定性

级别	内容	备注
A1	服务器产品可以 3×24 稳定运行	依赖于硬件设备： 1 运行产品的电脑性能稳定；

1. 运行需求

1.1. 外部接口

级别	内容	备注
A1	需要连接 RA 服务器	