# 江南科友SRJ1401、SJJ1817

# 1、支持算法

支持产生临时密钥对：RSA1024、RSA2048、SM2、P256、P384、P521；

支持RSA PKCS#1 V1.5解密；支持RSA Raw签名；

支持SM2解密；支持SM2签名；

支持ECDSA签名。

# 2、部署方法

## windows环境

* **定义**

**{netcaSys}**: 在32位系统上是指C:\Windows\System32, 在64位系统上是指C:\Windows\SysWOW64.

**{netcaSys64}：**C:\Windows\System32

（64位的操作系统需要部署win32+win64两种配置）

32位

|  |  |  |
| --- | --- | --- |
| 文件名称 | SVN路径 | 部署方法 |
| srj1401DevAPI.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/设备接口规范/Windows/x32/srj1401DevAPI.dll | 1、重命名为srj1401DevAPI.dll。  2、放到{netcaSys}。 |
| pkcs11.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Windows/SRJ1401PKCS11Test/p11win32/pkcs11.dll | 1. 重命名为srj1401pkcs11.dll。 2. 放到{netcaSys}。 |
| srj1401Hsm.conf | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/设备接口规范/Windows/x32/srj1401Hsm.conf | 1. 修改srj1401Hsm.conf 文件中的ipAddrOfCenterSecuSvr01（加密机的ip地址）项和portOfCenterSecuSvr01（加密机的端口）。 2. 在C:\目录下，建立一个文件夹nfast，在nfast建立文件etc，将srj1401Hsm.conf放到etc。 |
| UnionSRJ1401Prov.dll | <http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/winX86/设备驱动/>江南科友/UnionSRJ1401Prov.dll | 1、放到{netcaSys}。 |
| SRJ1401.reg | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX86/设备驱动/江南科友/SRJ1401.reg | 1. 修改注册表路径。32位系统的路径：[HKEY\_LOCAL\_MACHINE\SOFTWARE\NETCA\PKI\Devices\SRJ1401]；64位系统的路径：[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\NETCA\PKI\Devices\SRJ1401] 2. 修改dllpath项。指定UnionSRJ1401Prov.dll的路径。 3. 修改SM2KeyPairStatus项、RSAKeyPairStatus项、ECCKeyPairStatus项。   通过运行GetKeypairStatus\_SRJ1401.exe产生一个keypairStatus文件，这个文件记录了SM2KeyPairStatus、RSAKeyPairStatus、ECCKeyPairStatus的值。   1. 运行SRJ1401.reg。 |

64位

|  |  |  |
| --- | --- | --- |
| 文件名称 | SVN路径 | 部署方法 |
| srj1401DevAPI.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/设备接口规范/Windows/x64/srj1401DevAPI.dll | 1、重命名为srj1401DevAPI.dll。  2、放到{netcaSys64}。 |
| pkcs11.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Windows/SRJ1401PKCS11Test/p11win64/pkcs11.dll | 1. 重命名为srj1401pkcs11.dll。 2. 放到{ netcaSys64}。 |
| srj1401Hsm.conf | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/设备接口规范/Windows/x32/srj1401Hsm.conf | 1. 修改srj1401Hsm.conf 文件中的ipAddrOfCenterSecuSvr01（加密机的ip地址）项和portOfCenterSecuSvr01（加密机的端口）。 2. 在C:\目录下，建立一个文件夹nfast，在nfast建立文件etc，将srj1401Hsm.conf放到etc。 |
| UnionSRJ1401Prov.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX64/设备驱动/江南科友/UnionSRJ1401Prov.dll | 1、放到{ netcaSys64}。 |
| SRJ1401.reg | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX64/设备驱动/江南科友/SRJ1401.reg | 1. 修改注册表路径。64位系统的路径：[HKEY\_LOCAL\_MACHINE\SOFTWARE\NETCA\PKI\Devices\SRJ1401] 2. 修改dllpath项。指定UnionSRJ1401Prov.dll的路径。 3. 修改SM2KeyPairStatus项、RSAKeyPairStatus项、ECCKeyPairStatus项。   通过运行GetKeypairStatus\_SRJ1401.exe产生一个keypairStatus文件，这个文件记录了SM2KeyPairStatus、RSAKeyPairStatus、ECCKeyPairStatus的值。   1. 运行SRJ1401.reg。 |

## 2.2 linux环境

32位

|  |  |  |
| --- | --- | --- |
| 文件名称 | SVN路径 | 部署方法 |
| libsrj1401DevAPI.32bit.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/设备接口规范/Linux/DevAPI/WZTAPI/libsrj1401DevAPI.32bit.so | 1、重命名为libsrj1401DevAPI.so。  2、放到${LD\_LIBRARY\_PATH}。 |
| libUnionPkcs11API.32bit.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Linux/wzt.p11lib/nfast/lib/libUnionPkcs11API.32bit.so | 1. 重命名为libsrj1401pkcs11.so。 2. 放到${LD\_LIBRARY\_PATH}。 |
| srj1401Hsm.conf | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Linux/wzt.p11lib/nfast/etc/srj1401Hsm.conf | 1. 修改srj1401Hsm.conf 文件中的ipAddrOfCenterSecuSvr01（加密机的ip地址）项和portOfCenterSecuSvr01（加密机的端口）。 2. 在/root目录下，新建文件夹nfast，在/root/nfast新建文件夹etc，将srj1401Hsm.conf放到etc。 |
| libsrj1401prov.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX86/设备动态库/江南科友/libsrj1401prov.so | 1、放到${LD\_LIBRARY\_PATH}。 |
| DeviceStore\_srj1401 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX86/设备动态库/江南科友/DeviceStore\_srj1401 | 1. 修改sopath项。指定libsrj1401prov.so 的路径。 2. 打开/etc/.NETCA/DeviceStore文件，把DeviceStore\_srj1401的内容拷贝到DeviceStore后面 |
| SRJ1401KeyPairStatus | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX86/设备动态库/江南科友/SRJ1401KeyPairStatus | 1. 修改SM2KeyPairStatus项、RSAKeyPairStatus项、ECCKeyPairStatus项。 2. 通过运行GetKeypairStatusSRJ1401产生一个keypairStatus文件，这个文件记录了SM2KeyPairStatus、RSAKeyPairStatus、ECCKeyPairStatus的值。 3. 将SRJ1401KeyPairStatus拷贝到/etc/.NETCA/目录下。 |

64位

|  |  |  |
| --- | --- | --- |
| 文件名称 | SVN路径 | 部署方法 |
| libsrj1401DevAPI.64bit.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/设备接口规范/Linux/DevAPI/WZTAPI/libsrj1401DevAPI.64bit.so | 1、重命名为libsrj1401DevAPI.so。  2、放到${LD\_LIBRARY\_PATH}。 |
| libUnionPkcs11API.64bit.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Linux/wzt.p11lib/nfast/lib/libUnionPkcs11API.64bit.so | 1. 重命名为libsrj1401pkcs11.so。 2. 放到${LD\_LIBRARY\_PATH}。 |
| srj1401Hsm.conf | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Linux/wzt.p11lib/nfast/etc/srj1401Hsm.conf | 1. 修改srj1401Hsm.conf 文件中的ipAddrOfCenterSecuSvr01（加密机的ip地址）项和portOfCenterSecuSvr01（加密机的端口）。 2. 在/root目录下，新建文件夹nfast，在/root/nfast新建文件夹etc，将srj1401Hsm.conf放到etc。 |
| libsrj1401prov.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX64/设备动态库/江南科友/libsrj1401prov.so | 1、放到${LD\_LIBRARY\_PATH}。 |
| DeviceStore\_srj1401 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX64/设备动态库/江南科友/DeviceStore\_srj1401 | 1. 修改sopath项。指定libsrj1401prov.so 的路径。 2. 打开/etc/.NETCA/DeviceStore64文件，把DeviceStore\_srj1401的内容拷贝到DeviceStore后面 |
| SRJ1401KeyPairStatus | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX86/设备动态库/江南科友/SRJ1401KeyPairStatus | 1. 修改SM2KeyPairStatus项、RSAKeyPairStatus项、ECCKeyPairStatus项。 2. 通过运行GetKeypairStatusSRJ1401产生一个keypairStatus文件，这个文件记录了SM2KeyPairStatus、RSAKeyPairStatus、ECCKeyPairStatus的值。 3. 将SRJ1401KeyPairStatus拷贝到/etc/.NETCA/目录下。 |

# 江南科友SJJ1817-G

# 1、区别

功能：与SRJ1401型号加密机相比，SJJ1817-G加密机不支持pkcs11接口，支持的算法和部署方法大体一致。

# 2、部署方法

## windows环境

* **定义**

**{netcaSys}**: 在32位系统上是指{sys}, 在64位系统上是指{syswow64}.

（64位的操作系统需要部署win32+win64两种配置）

32位

|  |  |  |
| --- | --- | --- |
| 文件名称 | SVN路径 | 部署方法 |
| srj1401DevAPI.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/扩展接口SDFX/win\_lib/win32/srj1401DevAPI.dll | 1、重命名为srj1401DevAPI.dll。  2、放到{netcaSys}。 |
| pkcs11.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Windows/SRJ1401PKCS11Test/p11win32/pkcs11.dll | 1. 重命名为srj1401pkcs11.dll。 2. 放到{netcaSys}。 |
| srj1401Hsm.conf | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/设备接口规范/Windows/x32/srj1401Hsm.conf | 1. 修改srj1401Hsm.conf 文件中的ipAddrOfCenterSecuSvr01（加密机的ip地址）项和portOfCenterSecuSvr01（加密机的端口）。 2. 在C:\目录下，建立一个文件夹nfast，在nfast建立文件etc，将srj1401Hsm.conf放到etc。 |
| UnionSRJ1401Prov.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX86/设备驱动/江南科友/SJJ1817-G/UnionSRJ1401Prov.dll | 1、放到{netcaSys}。 |
| SRJ1401.reg | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX86/设备驱动/江南科友/SJJ1817-G/SRJ1401.reg | 1. 修改注册表路径。32位系统的路径：[HKEY\_LOCAL\_MACHINE\SOFTWARE\NETCA\PKI\Devices\SRJ1401]；64位系统的路径：[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\NETCA\PKI\Devices\SRJ1401] 2. 修改dllpath项。指定UnionSRJ1401Prov.dll的路径。 3. 修改SM2KeyPairStatus项、RSAKeyPairStatus项、ECCKeyPairStatus项。   通过运行GetKeypairStatus\_SRJ1401.exe产生一个keypairStatus文件，这个文件记录了SM2KeyPairStatus、RSAKeyPairStatus、ECCKeyPairStatus的值。   1. 运行SRJ1401.reg。 |

64位

|  |  |  |
| --- | --- | --- |
| 文件名称 | SVN路径 | 部署方法 |
| srj1401DevAPI.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/扩展接口SDFX/win\_lib/win64/srj1401DevAPI.dll | 1、重命名为srj1401DevAPI.dll。  2、放到{netcaSys}。 |
| pkcs11.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Windows/SRJ1401PKCS11Test/p11win64/pkcs11.dll | 1. 重命名为srj1401pkcs11.dll。 2. 放到{netcaSys}。 |
| srj1401Hsm.conf | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/设备接口规范/Windows/x32/srj1401Hsm.conf | 1. 修改srj1401Hsm.conf 文件中的ipAddrOfCenterSecuSvr01（加密机的ip地址）项和portOfCenterSecuSvr01（加密机的端口）。 2. 在C:\目录下，建立一个文件夹nfast，在nfast建立文件etc，将srj1401Hsm.conf放到etc。 |
| UnionSRJ1401Prov.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX64/设备驱动/江南科友/SJJ1817-G/UnionSRJ1401Prov.dll | 1、放到{netcaSys}。 |
| SRJ1401.reg | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX64/设备驱动/江南科友/SJJ1817-G/SRJ1401.reg | 1. 修改注册表路径。64位系统的路径：[HKEY\_LOCAL\_MACHINE\SOFTWARE\NETCA\PKI\Devices\SRJ1401] 2. 修改dllpath项。指定UnionSRJ1401Prov.dll的路径。 3. 修改SM2KeyPairStatus项、RSAKeyPairStatus项、ECCKeyPairStatus项。   通过运行GetKeypairStatus\_SRJ1401.exe产生一个keypairStatus文件，这个文件记录了SM2KeyPairStatus、RSAKeyPairStatus、ECCKeyPairStatus的值。   1. 运行SRJ1401.reg。 |

## 2.2 linux环境

32位

|  |  |  |
| --- | --- | --- |
| 文件名称 | SVN路径 | 部署方法 |
| libsrj1401DevAPI.32bit.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/扩展接口SDFX/linux\_lib/libsrj1401DevAPI.32bit.so | 1、重命名为libsrj1401DevAPI.so。  2、放到${LD\_LIBRARY\_PATH}。 |
| libUnionPkcs11API.32bit.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Linux/wzt.p11lib/nfast/lib/libUnionPkcs11API.32bit.so | 1. 重命名为libsrj1401pkcs11.so。 2. 放到${LD\_LIBRARY\_PATH}。 |
| srj1401Hsm.conf | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Linux/wzt.p11lib/nfast/etc/srj1401Hsm.conf | 1. 修改srj1401Hsm.conf 文件中的ipAddrOfCenterSecuSvr01（加密机的ip地址）项和portOfCenterSecuSvr01（加密机的端口）。 2. 在/root目录下，新建文件夹nfast，在/root/nfast新建文件夹etc，将srj1401Hsm.conf放到etc。 |
| libsrj1401prov.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX86/设备动态库/江南科友/SJJ1817-G/libsrj1401prov.so | 1、放到${LD\_LIBRARY\_PATH}。 |
| DeviceStore\_srj1401 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX86/设备动态库/江南科友/SJJ1817-G/DeviceStore\_srj1401 | 1. 修改sopath项。指定libsrj1401prov.so 的路径。 2. 打开/etc/.NETCA/DeviceStore文件，把DeviceStore\_srj1401的内容拷贝到DeviceStore后面 |
| SRJ1401KeyPairStatus | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX86/设备动态库/江南科友/SRJ1401KeyPairStatus | 1. 修改SM2KeyPairStatus项、RSAKeyPairStatus项、ECCKeyPairStatus项。 2. 通过运行GetKeypairStatusSRJ1401产生一个keypairStatus文件，这个文件记录了SM2KeyPairStatus、RSAKeyPairStatus、ECCKeyPairStatus的值。 3. 将SRJ1401KeyPairStatus拷贝到/etc/.NETCA/目录下。 |

64位

|  |  |  |
| --- | --- | --- |
| 文件名称 | SVN路径 | 部署方法 |
| libsrj1401DevAPI.64bit.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/扩展接口SDFX/linux\_lib/libsrj1401DevAPI.64bit.so | 1、重命名为libsrj1401DevAPI.so。  2、放到${LD\_LIBRARY\_PATH}。 |
| libUnionPkcs11API.64bit.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Linux/wzt.p11lib/nfast/lib/libUnionPkcs11API.64bit.so | 1. 重命名为libsrj1401pkcs11.so。 2. 放到${LD\_LIBRARY\_PATH}。 |
| srj1401Hsm.conf | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南科友/SRJ1401\_20160720/pkcs11/Linux/wzt.p11lib/nfast/etc/srj1401Hsm.conf | 1. 修改srj1401Hsm.conf 文件中的ipAddrOfCenterSecuSvr01（加密机的ip地址）项和portOfCenterSecuSvr01（加密机的端口）。 2. 在/root目录下，新建文件夹nfast，在/root/nfast新建文件夹etc，将srj1401Hsm.conf放到etc。 |
| libsrj1401prov.so | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX64/设备动态库/江南科友/SJJ1817-G/libsrj1401prov.so | 1、放到${LD\_LIBRARY\_PATH}。 |
| DeviceStore\_srj1401 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX64/设备动态库/江南科友/SJJ1817-G/DeviceStore\_srj1401 | 1. 修改sopath项。指定libsrj1401prov.so 的路径。 2. 打开/etc/.NETCA/DeviceStore64文件，把DeviceStore\_srj1401的内容拷贝到DeviceStore后面 |
| SRJ1401KeyPairStatus | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/linuxX86/设备动态库/江南科友/SRJ1401KeyPairStatus | 1. 修改SM2KeyPairStatus项、RSAKeyPairStatus项、ECCKeyPairStatus项。 2. 通过运行GetKeypairStatusSRJ1401产生一个keypairStatus文件，这个文件记录了SM2KeyPairStatus、RSAKeyPairStatus、ECCKeyPairStatus的值。 3. 将SRJ1401KeyPairStatus拷贝到/etc/.NETCA/目录下。 |