文件控制信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 文件名： | 软件安装配置清单 | | 受控状态 | √是 否 |
| 编 号： | NETCA-T01-PR03-GU07-RE01 | | 版本号 | V1.0 |
| 适用范围： | 本文件是《技术管理策略》的支持文件，为公司技术研发管理提供指引，适用于本公司。 | | | |
| 起 草 人： |  | 批 准 人： | 黄志平 | |
| 批准日期： | 2011年月日 | | | |
| 生效日期： | 2011年月日 | | | |

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。

3) 网证通安全中间件（NETCA\_Crypto）版本管理

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

NETCA\_Crypto(32位)打包说明清单

# 概述

网证通安全中间件（NETCA\_Crypto）配置文件说明清单对打包时的所需文件、文件的配置路径做了说明，打包时请参考该文档。

相关文件包括：

1). Crypto中间件文件;

2). COM文件

3). CSP签名文件

4). SecuInter

5). 安全环境

6). 注册表

## 定义说明

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

**{netcaPf}**：在32位系统上是指系统盘目录下的Program Files目录，在64位系统上是指系统盘目录下的Program Files (x86)目录。

{commonappdata}：

注：以上定义只适用于本文档，如果其它文档中出现同样的定义，以其它文档为准。

## 文件安装目录说明

把32位Crypto中间件文件DLL 、COM文件、CSP的NETCA\_CRYPTO\_RSACSP\_IMP.dll文件以及SecuInter.dll拷贝到**{netcaSys}**目录中；

CSP文件NETCA\_CRYPTO\_RSACSP.dll拷贝到“**{netcaPf}**\NETCA\NETCA\_Crypto\” 目录下。

注册COM文件，包括：NetcaPkiCom.dll和SecuInter.dll。注册命令：regsvr32 **{netcaSys}**\XXX.dll。

安全环境拷贝到目录拷贝到目录{commonappdata}\NETCA\certs。

注册表文件提取其中的内容。

## DLL文件签名要求

文档中，对DLL 文件（包括Crypto中间件文件、COM文件、CSP文件、SecuInter）是否需要签名做了说明，打包时，按照要求需要检查DLL文件是否符合要求。

## 文件版本升级说明

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本 | 日期 | 模块 | 文件 | 变更 | 版本更新功能 |
| V1.6.2 | 2013-03-28 | Crypto中间件文件 | NETCA\_CRYPTO.dll  NETCA\_CRYPTO\_UI.dll  NETCA\_CRYPTO\_UI\_RES\_1028.dll  NETCA\_CRYPTO\_UI\_RES\_1033.dll  NETCA\_CRYPTO\_UI\_RES\_2052.dll  NETCA\_LOG.dll  NETCA\_URL.dll  NETCA\_UTIL.dll | Modify | 中间件核心版本由V1.6.1升级到V1.6.2，增加对飞天502设备的支持；支持普华KM使用飞天SM2的Key；支持HTTP重定向；整合了新的证书验证API |
| COM文件 | npnetcapki.dll | Modify |  |
| 2013-04-27 | 设备DLL | FeiTianSM2Key.dll  NETCAKeyFTSM2.reg | Add | 增加设备飞天SM2 |
| 厂家驱动 | FTGM.dll | Add | 增加飞天SM2的厂家驱动，usbccid驱动手动安装，该版本不加入usbccid的驱动。 |
| Crypto中间件文件 | NETCA\_XML.dll | Modify | 升级到V2.1.0.0;  修复多次释放导致凭证崩溃的BUG |
| COM | NetcaPkiCom.dll | Modify | 升级到V1.6.2.0; 增加日志功能, 带时间戳签名的功, 手工设置CA证书验证用户证书的功能 |
| CSP | NETCA\_CRYPTO\_RSACSP\_IMP.dll | Modify | 升级到V1.1.0.0; 增加日志功能，并增加HMAC的支持 |
| 2013-05-18 |  |  |  | 将设备DLL、厂家驱动分离为单独的安装包 |
| 2013-05-27 | 安全环境 | trust | Modify | 增加ClassC的 证书链 |
| V1.7.0 | 2013-07-22 | COM | NetcaRAClientCom.dll | Add | 增加RA客户端COM，需注册该文件 |
| 2013-07-25 | Crypto | NETCA\_UTIL.dll、NETCA\_ASN1.dll、NETCA\_CRYPTO.dll、NETCA\_CRYPTO\_UI.dll | Modify | 升级到V1.7.0 |
| CSP | NETCA\_CRYPTO\_RSACSP\_IMP.dll | Modify |
| 注册表 | CertReqSubjectEncodeOption.reg | Add | 入根需要UTF8String编码 |
| 2013-07-29 | 注册表 | CertReqSubjectEncodeOption.reg | Delete | 已完成入根测试，标准版中不需要该项 |
| 2013-07-30 | 安全环境 | trust | Modify | 增加国密SM2的证书链 |
| 2013-08-02 | CRYPTO | NETCA\_UTIL.dll、NETCA\_CRYPTO.dll、NETCA\_XML.dll | Modify | 修正上个版本往设备中写数据失败的问题 |
| COM | NETCA\_XMLCOM.dll | Modify | 改正XML COM使用空串作为引用的URL导致崩溃的问题 |
| V1.7.1 | 2013-09-25 | CRYPTO | NETCA\_CRYPTO.dl | Modify | 1. 修正Key安装证书多次安装的问题; 2. 增加CheckPrivKey='True'过滤掉证书库里残余的证书 3. 增加密码缓存的一些配置 |
| 2013-11-25 | CRYPTO | NETCA\_LOG.dll | Modify | 升级到V2.0.0.1 |
| V1.7.2 | 2013-11-27 | CRYPTO | NETCA\_ASN1.dll | Modify | 升级到V1.2.14.0 |
| NETCA\_CRYPTO.dll | Modify | CRYPTO升级到V1.7.2.0，NetcaPKICertGetCertStringAtt ribute函数支持更多证书里的信息的获取，包括CRLDP里的CRL URL，AIA里的OCSP URL,DNS等。 |
| NETCA\_XML.dll | Modify | NETCA\_XML升级到V 2.1.3.0   1. XML签名修正SM2签名错误的BUG 2. XML签名修正BUG #636和BUG #637 |
| Crypto驱动检测配置文件 | record\_file\_crypto.ini | Add | 增加驱动检测的配置文件 |
| 2014-01-13 | CRYPTO | NETCA\_XML.dll | Modify | 修复Bug#731：文件URI中存在中文路径导致验证失败 |
| COM | NetcaPkiCom.dll | Modify | 1、增加了方法验证过期证书的签名  2、增加了清除密码缓存的功能  3、增加了从证书库里删除没私钥的证书的功能  4、Certificate对象的签名和解密使用NetcaPKIUIVerifyPassword来验证密码，和SignedData和EnvelopedData的保持一致。当前还不能做到完全一样 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| 2014-01-15 | CRYPTO | NETCA\_USBKeySvr.dll | Modify | 处理了NetcaPKICom调用的时候，进行卸载出现的内存读取问题。 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| 2014-03-27 | CRYPTO | NETCA\_XML.dll | Modify | 1、增加非UTF-8编码的XML的支持  2、修正XML签名的时候签名节点可能会出现两个XML签名的名字空间的BUG |
| NETCA\_XMLCOM.dll | Modify |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| 2014-04-02 | CRYPTO | NETCA\_XML.dll | Modify | 修正XML的非UTF-8编码解码问题。 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| V1.7.3 | 2014-05-23 | CRYPTO | NETCA\_CRYPTO.dll | Modify | 1、修复了大量内存泄漏问题  2、修正NetcaPKIMsgSignedDataVerify函数在多人签名的时候会返回重复的明文的BUG |
| NETCA\_CRYPTO\_UI.dll | Modify |
| NETCA\_URL.dll | Modify |
| npnetcapki.dll | Modify | 增加了与NetcaPkiCom.dll相比没有的一些方法和对象实现。 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| V1.8.0 | 2014-12-15 | CRYPTO | NETCA\_ASN1.dll | Modify | 1、增加了CCM、GCM和XTS等模式的实现  2、增加了CMAC的实现  3、修复证书句柄的并发问题  4、增加USB监控的函数，以便在没有KeyX的环境下使用  5、COM不再依赖于NETCA\_USBKeySvr.DLL来获取插拔事件。  6、JAVA和COM的SignedData增加自定义的签名属性和不签名属性的设置  7、增加纯JAVA的实现SignedData和数字信封 |
| NETCA\_CRYPTO.dll | Modify |
| NETCA\_UTIL.dll | Modify |
| NETCA\_XML.dll | Modify |
| NetcaPkiCom.dll | Modify |
| NetcaRSACNGProvider.dll | Add | 新增RSA和SM2的CNG |
| NetcaSM2CNGProvider.dll | Add |
| V1.8.1 | 2014-12-16 | CRYPTO | NETCA\_ASN1.dll | Modify | 1、允许配置使用其他的URL库  2、URL支持IPV6  3、SignedData支持添加和获取CRL  4、添加了PE文件(EXE和DLL等)的代码签名的功能  5、纯JAVA实现了RFC3161的时间戳  6、完善dotNet的实现，使之和Java的JNI提供基本相同的功能  7、修复PSSC类型不能连接的BUG  8、修复密码缓存导致崩溃的BUG  9、修复使用SHA-512算法产生错误时间戳请求的BUG |
| NETCA\_CRYPTO.dll | Modify |
| NETCA\_URL.dll | Modify |
| NETCA\_XML.dll | Modify |
| Crypto配置文件 | record\_file\_crypto.ini | Modify |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| V1.8.2 | 2015-03-16 | CRYPTO | NETCA\_ASN1.dll  NETCA\_CRYPTO.dll  NETCA\_URL.dll  NetcaJCrypto.dllNetcaSM2CNGProvider.dll  NETCA\_CRYPTO\_UI.dll | Modify | 1、增加S/MIME的实现  2、获取时间戳增加不带证书的响应的支持  3、修正获取HTTP分块响应出错的BUG  4、把两个CNG合并为一个  5、提供了纯软件实现的JAVA的SM2实现 |
|  | NetcaRSACNGProvider.dll | Delete | 合并到SM2CNG里面 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify |  |
| 2015-04-23 | 安全环境 | trust | Modify | 增加了SM2的证书链 |
| 注册表 | NetcaCryptoVersionInfo.reg | Add | 指明Crypto的版本 |
| 2015-06-05 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_CRYPTO\_UI.dll  NETCA\_CRYPTO\_UI\_RES\_1028.DLL  NETCA\_CRYPTO\_UI\_RES\_1033.dll  NETCA\_CRYPTO\_UI\_RES\_2052.DLL  NETCA\_URL.dll  NETCA\_XML.dll  NETCA\_XMLCOM.dll | Modify | 1、修正windows下的HTTPS访问的BUG（CRPT-10）  2、修正NETCA\_URL的HTTP重定向无法处理相对路径的BUG  3、修正XML签名在某些没意义的情况下，处理<http://www.w3.org/2000/09/xmldsig#enveloped-signature变换出错的BUG>  4、NETCA\_CRYPTO\_UI显示证书，增加证书链的显示和更多的扩展项的解析显示 |
|  | NetcaFormatObject.dll | Add | 用于扩展微软的证书显示，以便支持NETCA自定义扩展的显示 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | \ |
| 2015-06-19 | 可信站点 |  | Add |  |
| 2015-06-30 | 注册表 | NETCA\_CA.reg  NETCA\_ROOT.reg  NETCA\_SM2.reg | Add | 证书链 |
| 2015-07-08 | CRYPTO | NETCA\_CRYPTO.dll  NetcaPkiCom.dll  NETCA\_CRYPTO\_UI.dll  NetcaSM2CNGProvider.dll  NETCA\_CRYPTO\_UI\_RES\_1028.DLL  NETCA\_CRYPTO\_UI\_RES\_1033.dll  NETCA\_CRYPTO\_UI\_RES\_2052.DLL  NETCA\_USBKeySvr.dll | Modify | 1、时间增加毫秒的部分的处理  2、修正某些对称解密的时候，中间输入不是分组整数倍长度的解密错误  3、JAVA部分配合广通服公文加密项目，增加了SMIME和数字信封的直接使用C内存解析的处理  4、COM增加了获取设备密码重试次数的函数  5、CNG修正SSL双向认证崩溃的BUG  6、UI修复在某些系统上字体不为黑色的问题，并对界面进行了调整。  7、M 增加没有创建mapping view时，创建mapping view的功能 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | \ |
| 2015-08-10 | CRYPTO | NETCA\_CRYPTO.dll | Modify | 修复了BUG KX-488（系统首次安装keyx后，首次插入介质，keyx崩溃。） |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | \ |
| 2015-10-08 | CRYPTO | NetcaSM2CNGProvider.dll | / | 修改打包方式：   1. XP以及低于XP版本的操作系统不打包 2. 在64位操作，只注册64位的 |
| 2015-10-13 | CRYPTO | npnetcapki.dll | Modify | 修复获取证书扩展值失败的问题 |
| npnetcapki.reg | Modify | / |
| 1.8.3 | 2016-1-14 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_CRYPTO\_UI.dll  NETCA\_CRYPTO\_UI\_RES\_1028.DLL  NETCA\_CRYPTO\_UI\_RES\_1033.dll  NETCA\_CRYPTO\_UI\_RES\_2052.DLL  NETCA\_UTIL.dll  NETCA\_ASN1.dll  NetcaSM2CNGProvider.dll | Modify | 1、增加了C++的封装  2、增加ECDH的数字信封的支持，但是仅仅支持AES算法  3、CAdES增加CAdES-C、CAdES-X Long、CAdES-X Type 1、CAdES-X Type 2、CAdES-X Long Type 1 or 2和CAdES-A的支持  4、SignedData验证增加同时验证证书的功能  5、增加更多的证书项的获取，主要是补充完整RFC5280里的要求的主体项以及EV证书里的主体项  6、COM版本增加构造国密SM2标准的数字信封和SignedData  7、UI增加id-pkix-ocsp-nocheck的显示和修复KX-458  8、CNG解决[KX-708](http://192.168.0.123:8080/browse/KX-708)，开机后首次打开outlook2013，如果outlook指向的第一份邮件是加密邮件，输入PIN码后，outlook崩溃。 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| 2016-3-30 | CRYPTO | Netca.Pki.dll | Add | .net接口 |
| NetcaSM2CNGProvider.dll | / | 修改安装方式 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| 2.0 | 2016-4-12 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_ASN1.dll  NETCA\_UTIL.dll  NetcaPkiCom.dll | Modify | 1、增加SHA3的支持，但是没有找到签名相关的OID，因此SignedData还不能使用  2、增加配置信息和高层封装的函数  3、增加设备事件，仅Windows下有效  4、增加Adobe PDF的AdbeRevocationInfoArchival签名属性的处理  5、数字信封增加获取接收者信息的编码，以支持客户端解密对称密钥，服务端解对称加密的方式  6、修正一些BUG，包括PDFSP-9 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| 2.0.4 | 2016-5-16 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_ASN1.dll | Modify | 修正一些上个版本（2.0.1）引入的问题，比如:在某些情况下，使用OCSP验证证书状态会导致崩溃；解码某些Adobe RevocationInfoArchival会失败等等 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| 2.0.8 | 2016-6-15 | CRYPTO | NETCA\_CRYPTO.dll | Modify | 1、修正数字信封解密在直接设置对称密钥或者不解密的情况下还是需要有解密证书的BUG  2、修正验证证书的一些相关BUG，包括：过期验证，不验证时间验证OCSP等 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| 2.0.11 | 2016-9-1 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_ASN1.dll NetcaSM2CNGProvider.dll | Modify | 1、修正一些OCSP验证的错误  2、SignedData支持SHA-3相关的签名  3、CNG增加ECDSA的支持 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| 5.0.0 | 2016-11-14 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_ASN1.dll  NetcaSM2CNGProvider.dll  NETCA\_CRYPTO\_UI.dll  NETCA\_CRYPTO\_UI\_RES\_1028.DLL  NETCA\_CRYPTO\_UI\_RES\_1033.dll  NETCA\_CRYPTO\_UI\_RES\_2052.DLL  NetcaFormatObject.dll  NetcaRAClientCom.dll | Modify | 1、提供Android的版本  2、增加用户证书服务号、企业机构身份标识和个人身份标识等新扩展的支持  3、增加动态加载设备DLL的功能  4、非Windows系统增加设置验证密码回调函数的功能  5、优化了SHA3的速度 |
| Crypto配置文件 | record\_file\_crypto.ini | Modify | / |
| 2016-11-25 | CRYPTO | trust | Modify | 增加L1、L2、L3的证书链 |
|  | NETCA\_L3.reg  NETCA\_L2.reg  NETCA\_L2.reg | Add |
|  | 2016-12-29 | CRYPTO | NetcaSM2CNGProvider.dll | / | 64位系统，32位和64位的文件都需要注册。 |
| 5.1.0 | 2017-05-16 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_ASN1.dll  NETCA\_UTIL.dll  NETCA\_CRYPTO\_UI.dll  NETCA\_CRYPTO\_UI\_RES\_1028.DLL  NETCA\_CRYPTO\_UI\_RES\_1033.DLL  NETCA\_CRYPTO\_UI\_RES\_2052.DLL  NETCA\_UTIL.dll  record\_file\_crypto.ini | Modify | NETCA\_CRYPTO更新到版本5.1，主要修改如下：  1、SignedData和证书请求增加签名回调函数  2、证书路径和证书请求增加SHA3相关的签名算法支持  3、 区别几个 实体唯一标识的显示  4、修复keyx996，在解析新的自定义扩展个人身份标识和企业身份标识在一些机器上导致keyx崩溃的问题。 |
| 5.2.0 | 2017-06-28 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_ASN1.dll  NETCA\_URL.dll  NETCA\_UTIL.dll  NetcaSM2CNGProvider.dll  record\_file\_crypto.ini | Modify | 1、增加了格式化接口  2、修正了CAdES的一些实现错误  3、CAdES增加ETSI EN 319 122的支持  4、去除所有默认使用SHA-1的地方。  5、增加从设备和证书库里限制证书获取的配置  6、PE文件签名增加RFC3161时间戳和第二个签名的支持  7、纯JAVA增加基本的证书作废状态验证，并集成进证书路径验证  8、纯JAVA增加CAdES的支持  9、NETCA\_URL增加TLS的SNI扩展的支持 |
|  |  | NETCA\_CRYPTO\_UI.dll  record\_file\_crypto.ini | Modify | 修复证书ui常规页面当证书过期时显示错误的证书状态. |
| 5.2.1 | 2017-07-31 |  | NetcaPkiCom.dll record\_file\_crypto.ini | Modify | 添加设备格式化接口和获取状态属性, 去掉format返回值抛异常问题，改成不抛异常 |
| 2017-09-11 | CRYPTO | trust  NETCA\_L3.reg  NETCA\_L2.reg | Modify | 增加了CCS NETCA L2 Sub2 CA、CCS NETCA L2 Sub3 CA、CCS NETCA L3 Sub1 CA的中级证书 |
| 2017-10-20 | CRYPTO | CNCAPki.dll | Add | 增加应用开发接口COM |
|  | 2018-01-24 | CRYPTO | NetcaRAClientCom.dll | Modify | 修改删除密钥对接口，默认不谈UI。 |
| 5.5.0 | 2018.04.12 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_CRYPTO\_UI.dll  NETCA\_CRYPTO\_UI\_RES\_1028.DLL  NETCA\_CRYPTO\_UI\_RES\_1033.dll  NETCA\_CRYPTO\_UI\_RES\_2052.DLL  NetcaRAClientCom.dll  NetcaPkiCom.dll  NETCA\_ASN1.dll  NETCA\_UTIL.dll  NetcaSM2CNGProvider.dll  record\_file\_crypto.ini | Modify | 1、MIME增加非ASCII码的支持  2、增加国际化Email的支持  3、通过个人证书库调用微软CSP，现在可以支持CNG和ECDSA  4、增加试验性的功能，允许设备接口多次初始化  5、COM和JAVA的JNI增加JOSE的支持  6、COM增加根据配置进行证书类型过滤的功能  7、增加试验性的python3的简单封装  8、增加注册证书接口 |
| 5.5.1 | 2018-05-09 | CRYPTO | NETCA\_CRYPTO.dll  NetcaPkiCom.dll  record\_file\_crypto.ini  NETCA\_L3.reg  NETCA\_SM2.reg  trust | Modify | NETCA\_CRYPTO.dll：  修复CRPT-81、CRPT-85和CRPT-86：  证书匹配条件InValidity不起作用，内置软件设备RC2 CBC实现的错误（仅限于int和long的长度不同的系统），数字信封解密RC4算法释放内存两次的问题  NetcaPkiCom.dll：增加Websocket的JSON RPC接口 |
| 5.6 | 2018-07-13 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_ASN1.dll  NETCA\_XMLCOM.dll  record\_file\_crypto.ini | Modify | 1、增加签证书、签CRL、签OCSP响应、构造时间戳响应等功能。  2、修正设备的提示信息字符串没有加锁操作的问题，这个问题导致了在多线程的环境下使用共享设备句柄进行SignedData签名可能会两次释放内存，从而程序崩溃。  3、增加不信任的证书库，也就是黑名单。同时验证证书的时候增加一个使用系统证书库的选项。 |
| 5.6 | 2018-09-30 | CRYPTO | NetcaSKF.dll | Add | 实现GMT0016的接口。 |
| 5.7 | 2018-11-16 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_ASN1.dll  NETCA\_UTIL.dll  NETCA\_URL.dll  NETCA\_CRYPTO\_UI\_RES\_2052.DLL  Netca.Pki.dll  record\_file\_crypto.ini | Modify | 1、增加了SM9的支持  2、对称加密算法增加CFB、OFB、FF1、FF3等模式  3、增加了ECMQV的密钥协商  4、增加一个试验性的新的url库，它不依赖于openssl和openldap，并可以支持国密SSL。这个库当前设置为安卓的默认url库  5、纯JAVA实现了PFX的构造和解密  6、修复5.6.2引入的NetcaPKICertVerifyCert在某些情况下会导致程序崩溃的BUG |
| NETCA\_URL2.dll  Turst文件 | Add |
| 2019.04.04 | CRYPTO | trust  NETCA\_SM2.reg | Modify | 添加新的证书链 |
| 2019-05-21 | CRYPTO | NetcaSKF.dll | Modify | 增加SKF\_ECCDecrypt接口 |
| 2019-05-24 | CRYPTO | NetcaSKF.dll | Modify | 增加SKF\_WaitForDevEvent接口 |
| 2019-7-22 | CRYPTO | trust  NETCA\_SM2.reg | Modify | 删除SM2 L1相关证书。 |
| 2019-12-3 | CRYPTO | trust | Modify | 添加企业级CA证书链 |
| NETCA\_SM2LA1.reg | Add | 添加企业级CA证书链 |
| 5.8 | 2019-12-9 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_ASN1.dll  NETCA\_UTIL.dll  NETCA\_URL2.dll  NETCA\_LOG.dll  record\_file\_crypto.ini | Modify | NETCA\_CRYPTO更新到5.8，主要修改如下：  1、随机数发生器允许配置直接使用设备产生的随机数，并可以配置进行随机数测试  2、允许配置使用其他设备进行公钥运算，尤其是在验证证书签名的时候  3、增加SignedAndEnvelopedData的支持，包括C和纯JAVA  4、增加PKCS#8的私钥格式的支持  5、纯JAVA增加JOSE的支持  6、修复获取证书非DER编码的时候，由于指针转换错误导致在某些系统中崩溃的BUG  7、NETCA\_URL2修复URL中使用IPV6地址解析错误的BUG，支持断点续传和文件上传，增加TLS1.3的支持，添加日志 |
| 2019-12-13 | CRYPTO | trust | Modify | 将企业CA证书链从标准版中去除 |
| NETCA\_SM2LA1.reg | Delete |
| 2020.01.17 | CRYPTO | NETCA\_CRYPTO\_UI.dll | Modify | 修复多浏览器弹密码框的问题 |
| NETCA\_URL2.dll | Modify | 1、增加HTTPS 2.0的支持  2、修正TLS1.3因序列号用错导致加密出错的BUG  3、增加LDAPS的支持 |
| record\_file\_crypto.ini | Modify |  |
| 2020-02-28 | CRYPTO | NetcaSKF.dll | Modify | 修复LoadLibrary卡住问题 |
| 2020-03-10 | CRYPTO | NetcaSKF.dll | Modify | 修复FreeLibrary奔溃问题 |
| 5.9 | 2020-03-13 | CRYPTO | NETCA\_ASN1.dll  NETCA\_CRYPTO.dll  NetcaRAClientCom.dll | Modify | 1、增加一种新的KM加密保护加密私钥的数字信封的方式的支持  2、验证证书可以直接设置CRL句柄，以提高运行速度  3、带签名属性且不带原文的签名，可以直接设置Hash值来创建 |
| NetcaSAF.dll | Add | 增加GM/T 0019的实现 |
| 2020-03-18 | CRYPTO | NetcaSKF.dll | Modify | 考虑到中间件会一直使用，不释放监控设备函数的回调参数上下文内存 |
| 5.10 | 2020.5.29 | CRYPTO | NETCA\_ASN1.dll  NETCA\_CRYPTO.dll  record\_file\_crypto.ini | Modify | 1、支持GM/T 0031和GB/T 38540的电子印章和电子签章，包括C和纯JAVA  2、支持PKCS#5第二版使用口令导出密钥进行加密的EncryptedData，包括C和纯JAVA  3、KM的加密加密私钥的数字信封支持SM4算法  4、使用回调对象的JNI签名和解密，提供IGetErrorMessage接口来获取错误描述 |
| 2020.06.24 | CRYPTO | NETCA\_CRYPTO.dll  record\_file\_crypto.ini | Modify | NETCA\_CRYPTO更新到5.10.1，修复5.10.0引入的ImportOnlyEncKeypair=0的设备安装证书失败的BUG |
| 2020.7.7 | CRYPTO | NetcaRAClientCom.dll  record\_file\_crypto.ini | Modify | 更新到V1.2.2.7 增加接口：判断Key支持产生哪些算法的密钥对。 |
| 5.10.2 | 2020.09.23 | CRYPTO | NETCA\_URL2.dll | Modify | 更新netca\_url2到1.5.2版本  主要修改如下：  1、增加UDP的支持  2、增加DNS的实现  3、修正LDAP过滤表达式解析的问题  4、LDAP增加一次返回一条记录的迭代方法 |
| 5.10.3 | 2020.09.28 | CRYPTO | NETCA\_CRYPTO.dll  record\_file\_crypto.ini | Modify | NETCA\_CRYPTO更新到5.10.3，主要修改如下：   1、修复SignedData和EnvelopedData的内存泄漏问题  2、NetcaPKISelectCert默认去掉重复的证书 |
| 5.11 | 2020.11.08 | CRYPTO | NETCA\_ASN1.dll  NETCA\_CRYPTO.dll  NETCA\_UTIL.dll | Modify | NETCA\_CRYPTO更新到5.11，主要修改如下：  1、纯JAVA增加了很多算法的实现，包括：SHA-1、SHA-2、HMAC、AES、SM4、RSA、ECDSA、ECDH、SM9等  2、C部分增加了使用SCVP协议进行委托路径构造和委托路径验证  3、纯JAVA增加了JSON序列化功能  4、根据检测做了相应修改 |
| 2020.11.18 | CRYPTO | NETCA\_CRYPTO\_UI.dll  NETCA\_CRYPTO\_UI\_RES\_1028.DLL  NETCA\_CRYPTO\_UI\_RES\_1033.dll  NETCA\_CRYPTO\_UI\_RES\_2052.DLL | Modify | 1.证书选择框 添加了单位  2.调整了字段显示顺序 |
| 2020.11.21 | CRYPTO | NETCA\_ASN1.dll | Modify | NETCA\_CRYPTO更新到5.11.4，主要修改如下：  1、把netcajce.jar拆分为：netcajce.jar和netcapki-softwarejce.jar。前者使用JNI，支持JAVA 6，后者使用纯JAVA，支持JAVA 8。  2、完善纯JAVA的JCE，增加了大量算法支持和私钥支持，现在是个全功能的JCE  3、修复YSB-37。SignedData存在多余数据的时候导致程序崩溃问题  4、修复纯JAVA的net.netca.pki.algorithm.blockcipher.mode下的填充问题 |
| 5.11.8 | 2021.2.7 | CRYPTO | NETCA\_CRYPTO.dll  NETCA\_URL2.dll | Modify | 1、内置的软设备、openssl软设备、软证书，修复了在某些情况下，SM2解密失败的BUG。BUG：关于SM2解密失败的BUG，如果是原来使用内置的软设备的加密的结果都可以正常解密。默认使NetcaPKICertGetCertPublicKey得到的公钥句柄进行加密是使用内置的软设备进行加密的，除非配置指定使用特定的密码设备。使用纯JAVA的SM2加密，或者其他公司实现的SM2加密会有一定的概率解密失败。原因是KDF产生的数据全0判断错误。  2、netca\_url2修复在遇到TLS空会话ID握手失败的BUG  3、在NETCA\_CRYPTO层增加了HTTP代理支持，但WinInet实现除外，当前还是实现系统的代理  4、JSON序列化修复自定义序列化编码实现错误等问题，并增加List、Set和Map等的支持  5、SM4-CBC的OID可配置 |

# 32位版本配置信息

## 32位Crypto中间件文件、COM文件、CSP文件和SecuInter文件

以下文件如果是32位系统打包在{sys}目录中，如果是64位系统，打包在{syswow64}目录中。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 文件类别 | 文件名 | 版本 | 是否需要签名 | 说明 | SVN路径 |
| Crypto中间件文件 | libgmp-10.dll | / | N | 无版本信息 | <http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/winX86/动态库/Crypto> |
| NETCA\_ASN1.dll | 1.9.0.0 | **Y** |  |
| NETCA\_CRYPTO.dll | 5.11.8.0 | **Y** | 中间件核心动态库文件 |
| NETCA\_CRYPTO\_UI.dll | 1.2.9.5 | **Y** | UI核心文件 |
| NETCA\_CRYPTO\_UI\_RES\_1028.DLL | 1.2.5.1 | **Y** | 繁体中文支持文件 |
| NETCA\_CRYPTO\_UI\_RES\_1033.dll | 1.2.5.1 | **Y** | 英文支持文件 |
| NETCA\_CRYPTO\_UI\_RES\_2052.DLL | 1.2.5.1 | **Y** | 简体中文支持文件 |
| NETCA\_LOG.dll | 2.3.0.0 | **Y** | 日志文件 |
| NETCA\_URL.dll | 1.0.12.0 | **Y** |  |
| NETCA\_USBKeySvr.dll | 1.0.4.0 | **Y** |  |
| NETCA\_UTIL.dll | 2.7.1.0 | **Y** |  |
| NETCA\_XML.dll | 2.2.1.0 | **Y** | XML支持文件 |
| NetcaFormatObject.dll | 1.0.0.5 | **Y** | 显示证书自定义的扩展和证书链信息  注册的命令为：regsvr32 **{netcaSys}**\ NetcaFormatObject.dll |
| NETCA\_URL2.dll | V1.6.0.0 | Y |  |
| COM | NetcaPkiCom.dll | 2.0.4.0 | **Y** | 注册的命令为：regsvr32 **{netcaSys}**\ NetcaPkiCom.dll | <http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/winX86/动态库/COM> |
| NETCA\_XMLCOM.dll | 1.0.3.1 | **Y** | 注册的命令为：regsvr32 **{netcaSys}**\NETCA\_XMLCOM.dll |
| NetcaRAClientCom.dll | 1.2.2.7 | **Y** | 拷贝到**{netcaSys}**目录下; regsvr32 **{netcaSys}**\ NetcaRAClientCom.dll |
| LittleUtils.dll | 1.1.0.0 | Y | 拷贝到**{netcaSys}**目录下; regsvr32 **{netcaSys}**\ LittleUtils.dll |
| npnetcapki.dll | 1.0.2.1 | **Y** | 拷贝到**{netcaSys}**目录下 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX86/动态库/Chrome |
| npnetcapki.reg | / | / | npnetcapki.dll的注册表 |
| CNCAPki.dll | 1.0.2.0 | Y | 拷贝到**{netcaSys}**目录下; regsvr32 **{netcaSys}**\ CNCAPki.dll | http://192.168.0.11:8081/svn/rdrelease/软件发布/南方电网/应用开发接口/com接口/x86/ |
| CNG | NetcaSM2CNGProvider.dll | 1.7.0.0 | **Y** | 注册的命令为：regsvr32 **{netcaSys}**\ NetcaSM2CNGProvider.dll  1、在XP、Server2000、Server2003的操作系统下不打包这个文件 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX86/CSP |
| dotNet | Netca.Pki.dll | 5.7.0.0 | **N** | 拷贝到**{netcaSys}**目录下 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX86/动态库/dotNet/ |
| CSP文件 | NETCA\_CRYPTO\_RSACSP.dll | 1.0.1.0 | N | 拷贝到**{netcaSys}**目录下 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX86/CSP |
| NETCA CRYPTO RSA Cryptographic Provider.reg |  | N | **注册表文件无需拷贝**，只需提取其中内容 |
| NETCA\_CRYPTO\_RSACSP\_IMP.dll | 1.1.2.0 | **Y** | 拷贝到**{netcaSys}**目录 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX86/动态库/Crypto |
| SecuInter | SecuInter.dll | 4.1.0.1 | **Y** | 注册命令：regsvr32 **{netcaSys}**\ SecuInter.dll | <http://192.168.0.11:8081/svn/rdrelease/软件发布/SecuInter/4.1/x86> |
| SKF | NetcaSKF.dll | 1.0.5.23 | **Y** | 拷贝到**{netcaSys}**目录 | <http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/> current/winX86/动态库/SKF/ |
| SAF | NetcaSAF.dll | 1.0.0.1 | **Y** | 拷贝到**{netcaSys}**目录 | <http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/> current/winX86/动态库/SAF/ |
| 安全环境 | trust | SVN版本号：  48440 | N | 拷贝到目录  {commonappdata}\NETCA\certs | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/安全环境 |
| Crypto驱动检测配置文件 | record\_file\_crypto.ini | / | N | **{netcaPf}**\NETCA\NETCA\_Crypto\ | <http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/winX86/动态库/Crypto> |
| Crypto版本的注册表 | NetcaCryptoVersionInfo.reg | / | / | **Crypto版本的注册表** | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX86/注册表/NetcaCryptoVersionInfo.reg |

## COM的ProgID

|  |  |
| --- | --- |
| COM名称 | ProgID |
| NetcaPKICom.dll | NetcaPki.Certificate |
| NetcaRAClientCom.dll | NetcaRAClientCom.Key |
| NETCA\_XMLCOM.dll | NETCA\_XMLCOM.Document |
| npnetcapki.dll | npnetcapki.Certificate |
| SecuInter.dll | SecuInter.Signature |

# 可信站点

将下列地址加入可信站点：

[http://\*.cnca.net](http://121.33.212.110)

[https://\*.cnca.net](https://*.cnca.net)

[http://\*.netca.net](http://*.netca.net)

[https://\*.netca.net](https://*.netca.net)

[http://\*.netca.net.cn](http://*.netca.net.cn)

[https://\*.netca.net.cn](https://*.netca.net.cn)

[https://\*.netca.mobi](https://*.netca.mobi)

[http://\*.netca.mobi](http://*.netca.mobi)

# 4 证书链（注册表）

|  |  |  |
| --- | --- | --- |
| 文件名 | SVN位置 | 说明 |
| NETCA\_CA.reg | <http://192.168.0.11:8081/svn/rdrelease/软件发布/统一介质管理工具/current/发布版/证书链> | NETCA证书链 |
| NETCA\_Root.reg |
| NETCA\_SM2.reg |
| NETCA\_L1.reg |
| NETCA\_L2.reg |
| NETCA\_L3.reg |