Novell Developer Kit

www.novell.com

October 11, 2006

NOVELL CERTIFICATE SERVER™
APIS — OVERVIEW

Novell®

Novell Trademarks

For a list of Novell trademarks, see Trademarks (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

The Novell® Certificate Server™ APIs enable you to deploy a public key infrastructure (PKI) service within your organization. Once installed, the PKI service allows you to create, manage, and access X.509 certificates. These APIs help you use this functionality to further enhance or customize your security solutions without rewriting your own technology.

This guide contains the following sections:

Audience

This guide is intended for Java and C developers who desire to implement Novell Certificate Server functionality on their applications.

Feedback

We want to hear your comments and suggestions about this manual. Please use the User Comments feature at the bottom of each page of the online documentation and enter your comments there.

Documentation Updates

For the most recent version of this guide, see Novell Certificate Server Libraries for C (http://developer.novell.com/ndk/ncslib.htm).

Additional Documentation

For more comprehensive background information about setting up, managing, and troubleshooting this service, see the Novell Certificate Server Administration Guide (http://www.novell.com/documentation/lg/crt221ad/index.html).

The new Certificate Server functionality runs only on the same platforms as eDirectory 8.7 (see Novell eDirectory 8.7 System Requirements (http://www.novell.com/products/edirectory/sysreqs.html)

For Certificate Server source code projects, visit Forge Project: Novell Certificate Server Libraries for C (http://forge.novell.com/modules/xfmod/project/?ncslib) and Forge Project: Novell Certificate Server Classes for Java (http://forge.novell.com/modules/xfmod/project/?ncsjava).

For Certificate Server sample code, see Novell Certificate Server Libraries for C (../../../samplecode/ncslib_sample/index.htm).

For help with Certificate Server problems or questions, visit the Novell NCSLIB Support Forum (http://developer-forums.novell.com/group/novell.devsup.ncslib/readerNoFrame.tpt/@thread@first).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux or UNIX, should use forward slashes as required by your software.

Getting Started

1

The Novell® Certificate Server™ APIs are currently provided in the C and Java programming languages to provide the best cross-platform support for all platforms integrated with eDirectory™. The Certificate Server APIs are summarized below:

Table 1-1 *Novell Certificate Server APIs*

API Name and Documentation Link	Description	Dependencies	Supported Platforms
Certificate Server Library for C Version 1 (NWPKI) (http://forge.novell.com/modules/xfcontent/private.php/ncslibv1/README.html)	**Novell Certificate Server Library for C** The original public key management API library that is deprecated See Section 1.1.1, "NWPKI API," on page 8.	See Novell Certificate Server 2.0 System Requirements (http://www.novell.com/products/certserver/sysreqs.html).	• NetWare® 5.0, 5.1, and 6 • Windows* NT*/2000/XP
NDK: Novell Certificate Server Library for C Version 2	**Novell Certificate Server Version 2** A new cross platform, directory-centered public key management C library that does not depend on a Novell Client See Section 1.1.2, "NPKI and NPKIT APIs," on page 9.	See Novell eDirectory™ 8.8 System Requirements (http://www.novell.com/products/edirectory/sysreqs.html).	• NetWare 5.1 SP4 • Windows NT/2000/XP • Red Hat* Linux* 7.1 or greater • Solaris* 7 or 8 • AIX* 4.3 or 5L
NDK: Novell Public Key Infrastructure Toolbox	**Novell Public Key Infrastructure Toolbox** A new cross platform, non-directory public key utility library See Section 1.1.2, "NPKI and NPKIT APIs," on page 9.	See "Dependencies".	• NetWare 5.1 SP4 • Windows NT/2000/XP • Red Hat Linux 7.1 or greater • Solaris 7 or 8 • AIX 4.3 or 5L

API Name and Documentation Link	Description	Dependencies	Supported Platforms
NDK: Novell Certificate Server Classes for Java	**Novell Java Public Key Infrastructure** A Java cross platform, non-directory public key utility library See Section 1.1.3, "JPKI API," on page 9. **NOTE:** The link to NDK Novell Certificate Server Classes for Java will not resolve in Adobe PDF format. To access this component, see Certificate Server Classes for Java (http://developer.novell.com/ndk/doc/ncsjava/jpki_enu/data/bktitle.html).	See Novell eDirectory 8.8 System Requirements (http://www.novell.com/products/edirectory/sysreqs.html).	• NetWare 5.1 SP4 • Windows NT/2000/XP • Red Hat Linux 7.1 or greater • Solaris 7 or 8 • AIX 4.3 or 5L

This section discusses the following topics:

- Section 1.1, "Certificate Server API Background," on page 8
- Section 1.2, "Benefits of Novell Certificate Server," on page 10
- Section 1.3, "Understanding Directory Objects and Attributes," on page 11

1.1 Certificate Server API Background

- Section 1.1.1, "NWPKI API," on page 8
- Section 1.1.2, "NPKI and NPKIT APIs," on page 9
- Section 1.1.3, "JPKI API," on page 9
- Section 1.1.4, "NICI Dependency," on page 9

1.1.1 NWPKI API

NWPKI is the original Novell Certificate Server Library for C API developed to enable public key management solutions on applications that require a Novell Client. NWPKI functions only on the Novell NetWare 5.0, 5.1 and 6, and Microsoft* Windows NT/2000/XP platforms.

Although Novell will continue to provide short term NWPKI API support, it is recommended that developers begin using either NPKI or NPKIT API libraries. Both of these new libraries eliminate the dependency upon the Novell Client and expand the array of platforms for which security services can be implemented as described below.

IMPORTANT: With the introduction of new Certificate Server APIs, the NWPKI API library will soon be deprecated.

1.1.2 NPKI and NPKIT APIs

The NPKI (Novell Certificate Server Version 2) and NPKIT (Novell Public Key Infrastructure Toolbox) APIs operate together to provide the same functionality as the old NWPKI API, but eliminate its dependency upon the Novell client. In other words, neither NPKI nor NPKIT require the Novell client.

The old functionary provided by NWPKI, which is not dependant on a directory service, has been moved to the NPKIT library, while the directory-dependant functionality can be found in the NPKI library. The new function names (prefaced by NPKI and NPKIT) allow the newer API version to run on the same machine as the old version for backward compatibility. In addition, both libraries have new functionality and enhanced capabilities as described in Table 1.

The new Certificate Server functions should be used by all new applications, as well as existing applications using any of the new functionality. The new Certificate Server functionality runs only on the same platforms as eDirectory 8.7 (see Novell eDirectory 8.7 System Requirements (http://www.novell.com/products/edirectory/sysreqs.html)).

NOTE: Existing programs will retain backward compatibility.

Other changes resulting from the introduction of the NPKI and NPKIT APIs include:

- Moving away from a single binary delivery to two new deliveries per platform as a means to provide support for functions that have a dependency on eDirectory (NPKI-prefaced) and those that do not (NPKIT-prefaced).
- Adding new functions to each API, with a major new section for encoding and decoding PKCS #12 certificates.

IMPORTANT: Both NPKI and NPKIT APIs should be downloaded and enabled together to obtain full Certificate Server functionality.

1.1.3 JPKI API

The *NDK: Novell Certificate Server Classes for Java* (JPKI) enable you to access the Certificate Server API directly from their Java programs. This API provides a JNI interface to the native Certificate Server API. The native API is supported on all eDirectory platforms.

1.1.4 NICI Dependency

All Novell Certificate Server APIs require the cryptography services of Novell International Cryptographic Infrastructure (NICI). NICI is the underlying cryptographic infrastructure that provides the cryptography for Novell Certificate Server and other Novell applications.

WARNING: Novell Certificate Server will not function if cryptography services are not fully installed.

To determine the current version of NICI that should be used to implement Certificate Server for your solutions, see the Dependencies section in Table 1.

NICI availability and cryptography strength is restricted if your network is located in an entity listed on the U.S. Government Restricted Party List or in a country with import controls on cryptography products or technologies.

For details about setting up, managing, and troubleshooting NICI, see the NICI Administration Guide (http://www.novell.com/documentation/lg/nici/pdfdoc/nici_admin_guide.pdf).

1.2 Benefits of Novell Certificate Server

Public key cryptography presents developers with unique security challenges. Depending upon which API you implement, Novell Certificate Server helps you meet these challenges in the following ways (see Table 1 for a review of the capabilities of each library):

- `Provides public key cryptography services on your network`

  You can create an Organizational Certificate Authority (CA) within your eDirectory tree, allowing you to issue an unlimited number of user and server certificates. You can also use the services of an external certificate authority, or use a combination of both as your needs dictate.

- `Controls the costs associated with obtaining key pairs and managing public key certificates`

  You can create an Organizational CA, generate unlimited key pairs, and issue unlimited public key certificates through the Organizational CA at no charge.

- `Allows public keys and public key certificates to be openly available while also protecting them against tampering`

  Key pairs are stored in eDirectory and can therefore leverage eDirectory replication and access control features.

- `Allows private keys to be accessible to only the software routines that use them for signing and decrypting operations`

  Private keys are encrypted by Novell International Crytographic Infrastructure (NICI) and made available only to the software routines using them for signing and decrypting operations.

- `Securely backs up private keys`

  Private keys are encrypted by NICI, stored in eDirectory, and backed up using standard eDirectory backup utilities.

- `Allows central administration of certificates using ConsoleOne®`

  A ConsoleOne snap-in allows the administrator to manage certificates issued from a Novell CA.

- `Allows users to manage their own certificates`

  Users can use the Novell Certificate Console utility to export keys for use in cryptography-enabled applications without requiring intervention by the system administrator.

- `Supports popular email clients and browsers`

  Novell Certificate Server allows you to create and manage industry standard user certificates for securing e-mail. Novell Certificate Server supports Microsoft Outlook98*, Outlook2000, Netscape* Messenger*, and other popular e-mail clients. It also supports both Netscape Navigator* and Microsoft Internet Explorer.

- `Supports Certificate Revocation Lists (CRL) and certificate chain verification`

Novell Certificate Server enables you to import CRLs into the directory. This allows users and administrators to validate certificates through ConsoleOne. Certificate chains can also be validated. This validation process starts at the root certificate and checks every certificate up to the trusted root.

1.3 Understanding Directory Objects and Attributes

To implement Certificate Server in your applications, you need to understand the following directory objects and attributes:

- Section 1.3.1, "Certificate Authorities," on page 11
- Section 1.3.2, "Server Certificates," on page 11
- Section 1.3.3, "User Certificates," on page 11

If you need more detailed information, see the Novell Certificate Server Administration Guide (http://www.novell.com/documentation/lg/crt221ad/index.html).

1.3.1 Certificate Authorities

Certificate Authority (CA) objects are required to generate new certificates. The functionality of a CA is hosted by a specific server and implemented by PKI server software.

The organizational CA is the organizational (or root) CA. Every eDirectory tree can have only one organizational CA object, and the organizational CA object must be created before subordinate CAs.

The organizational CA can be created and viewed in ConsoleOne. Organizational CA has one object: Organizational CA, an eDirectory object.

1.3.2 Server Certificates

A server can have multiple certificates, and the server's Secure Authentication Services (SAS) object maintains the list of these certificates. Server-based applications can use these certificates to enable encryption, such as Secure Socket Layer (SSL), Transport Layer Security (TLS), and Virtual Private Network (VPN) sessions.

Server certificates can be created and managed in ConsoleOne. Server certificates support applications on a given server that use keys and certificates; for example, Lightweight Directory Access Protocol (LDAP), BorderManager®.

Server certificates can be exported to and imported from a PKCS#12 file. This can be done through ConsoleOne.

1.3.3 User Certificates

Each user can have any number of certificates, and each certificate can have different key sizes and be customized for different uses, such as key encryption and digital signature. Applications are able to select from among available keys or use a key with a given nickname.

Once Certificate Server is installed, ConsoleOne can manage Novell user certificates. User certificates have the following attributes:

- Stored in the userCert attribute of the User object.
- Private keys are stored in secret store for the user.
- Public keys are stored directly in the certificate.
- Referenced by a nickname.
- Managed by ConsoleOne, which supports Novell certificates, and which provides basic support for other certificates installed through LDAP.

Updating Certificate Server APIs

2

This chapter is provided to help you replace Novell Certificate Server Version 1 with *NDK: Novell Certificate Server Library for C Version 2* and *NDK: Novell Public Key Infrastructure Toolbox*. Both files are required to update from Version 1.

Because Novell Certificate Server Version 1 (http://forge.novell.com/modules/xfcontent/private.php/ncslibv1/README.html) is being deprecated, new development and existing software, which implement the new functionality contained in Version 2 and PKI Toolbox, should use the new APIs. Existing programs will retain backward compatibility.

For more information about the differences between these API libraries, see Section 1.1.2, "NPKI and NPKIT APIs," on page 9. You can also find complete documentation for each of the Certificate Server libraries at:

- Certificate Server Library for C Version 1 (http://developer.novell.com/ndkservlets/ndkdownload?filename=unsupported/ncslibv1.zip&logentry=unsupported)

  IMPORTANT: This component is being deprecated and replaced with the following two Certificate Server components.

- NDK Certificate Server Library for C Version 2 (http://developer.novell.com/ndk/doc/ncslib/npki_enu/data/bktitle.html)
- Novell Public Key Infrastructure Toolbox (http://developer.novell.com/ndk/doc/ncslib/npkitenu/data/bktitle.html)

2.1 Converting from PKIAPI to NPKIAPI

Converting APIs from PKIAPI to NPKIAPI is relatively easy. Old functions in PKIAPI that were prefaced with NWPKI are now prefaced in NPKIAPI with NPKI. The NWx509 calls have been removed from NPKIAPI and their functionality is now part of NPKIT.

NWPKIVerifyCertificate and NWPKIIssuerSubjectNameMatch have been moved to NPKIT. Since NPKIAPI no longer requires the Novell Client, NWPKISetIdentity could not be ported to the newer APIs. (To reference documentation on these NWPKI functions, download the deprecated documentation at Novell Certificate Server Version 1 (http://developer.novell.com/ndkservlets/ndkdownload?filename=unsupported/ncslibv1.zip&logentry=unsupported).)

2.1.1 Updating Certificate Server Header Files

Certificate Server header files also have changed, as shown in the chart below:

Old Header File Name	New Header File Name
nwpki.h (DS specific functions)	npki.h
nwpkikey.h	npkikey.h
nwverify.h	nverify.h

Old Header File Name	New Header File Name
nwx509.h	NPKIT_x509.h
pkierr.h	No change
nwpki.imp	npki.imp
nwpki.h (Non-DS specific verify functions)	NPKIT_Verify.h
	NPKIT_PKCS12.h (New API functions)

2.1.2 Updating Verify Functions

The verify functions that were in PKIAPI have been ported to NPKIT. These versions of the APIs are eDirectory independent do not require a context.These functions are preceded with NPKIT_Verify.

The certificate revocation list (CRL) functions in NPKIT are preceded with NPKIT_CRL. The other NWx509 functions in NPKIT are now preceded with NPKIT_x509. The NPKIT CRL and NPKIT_x509 functions each require their own context. Below is a conversion table for quick reference.

NOTE: See the NPKIAPI or NPKIT documentation links for proper usage.

NWPKIAPI Functions	NPKIAPI Functions
NWPKICreateContext	NPKICreateContext
NWPKIFreeContext	NPKIFreeContext
None	NPKIVersionInfo*
NWPKISetTreeName	NPKISetTreeName
NWPKIDSLogin	NPKIDSLogin
NWPKISetIdentity**	No longer available
NWPKIDSLogout	NPKIDSLogout
None	NPKIDSConnectToAddress*[1]
None	NPKIConnectToIPAddress*
NWPKIDeleteDSObject	NPKIDeleteDSObject
NWPKIFindKeyGenServersForUser	NPKIFindKeyGenServersForUser
NWPKIFindServersInContext	NPKIFindServersInContext
NWPKIServerNames	NPKIServerNames
NWPKIFindOrganizationalCA	NPKIFindOrganizationalCA
NWPKIGetServerUTCTime	NPKIGetServerUTCTime
NWPKIGetHostServerDN	NPKIGetHostServerDN

NWPKIAPI Functions	NPKIAPI Functions
NWPKIGetServerCertificateStatus	NPKIGetServerCertificateStatus
NWPKIGetSASServiceName	NPKIGetSASServiceName
NWPKIGetServerInfo	NPKIGetServerInfo
NWPKIGetAlgorithmInfo	NPKIGetAlgorithmInfo
NWPKIGenerateCertificateFromCSR	NPKIGenerateCertificateFromCSR
NWPKICreateServerCertificate	NPKICreateServerCertificate
NWPKICSRInfo	NPKICSRInfo
NWPKICertInfo	NPKICertInfo
NWPKICreateUserCertificate	NPKICreateUserCertificate
NWPKIDeleteUserCertificate	NPKIDeleteUserCertificate
NWPKIReadAllNickNames	NPKIReadAllNickNames
NWPKINickName	NPKINickName
NWPKIStoreUserCertificate	NPKIStoreUserCertificate
None	NPKICertificateList*
None	NPKIStoreServerCertificatesFromCertificateList*
NWPKIFindUserCertificates	NPKIFindUserCertificates
NWPKIUserCertInfo	NPKIUserCertInfo
NWPKIImportServerKey	NPKIImportServerKey
NWPKIImportCAKey	NPKIImportCAKey
NWPKIExportUserKey	NPKIExportUserKey
NWPKIExportServerKey	NPKIExportServerKey
NWPKIExportCAKey	NPKIExportCAKey
NWPKICreateOrganizationalCA	NPKICreateOrganizationalCA
NWPKIGetServerCertificates	NPKIGetServerCertificates
NWPKIGetCACertificates	NPKIGetCACertificates
NWPKIChainCertInfo	NPKIChainCertInfo
NWPKIStoreServerCertificates	NPKIStoreServerCertificates
NWPKIFindServerCertificateNames	NPKIFindServerCertificateNames
NWPKIServerCertificateName	NPKIServerCertificateName
NWPKIGetWrappedServerKey	NPKIGetWrappedServerKey
NWPKIGetServerIPAndDNSInfo	NPKIGetServerIPAndDNSInfo
NWPKIGetServerIPAddress	NPKIGetServerIPAddress

NWPKIAPI Functions	NPKIAPI Functions
NWPKIGetServerDNSName	NPKIGetServerDNSName
NWPKICreateTrustedRootContainer	NPKICreateTrustedRootContainer
NWPKICreateTrustedRoot	NPKICreateTrustedRoot
NWPKIFindTrustedRootsInContext	NPKIFindTrustedRootsInContext
NWPKIGetTrustedRootInfo	NPKIGetTrustedRootInfo
NWPKIVerifyCertificateWithTrustedRoots	NPKIVerifyCertificateWithTrustedRoots
NWPKIVerifyCertChain	NPKIVerifyCertChain[1]
NWPKIVerifyCertChainWithCallback	NPKIVerifyCertChainWithCallback[1]
NWPKIGetHandleToUserKey	NPKIGetHandleToUserKey
NWPKIGetHandleToServerKey	NPKIGetHandleToServerKey

2.1.3 Converting x509 Functions

The follow conversion table shows the quick references for x509 functions:

NOTE: * indicates new functionality; function not yet documented.
** indicates that functionality is not available.

NWPKIAPI x509 Functions	NPKIT x509 Functions
None	NPKIT_Version*
NWx509CreateContext	NPKIT_x509CreateContext
NWx509FreeContext	NPKIT_x509FreeContext
NWx509DecodeCertificate	NPKIT_x509DecodeCertificate
NWx509GetExtensionData	NPKIT_x509GetExtensionData
NWx509BasicConstraintsInfo	NPKIT_x509BasicConstraintsInfo
NWx509KeyUsageInfo	NPKIT_x509KeyUsageInfo
NWx509SubjectAltNamesInfo	NPKIT_x509SubjectAltNamesInfo
NWx509SubjectAltName	NPKIT_x509SubjectAltName
NWx509IssuerAltNamesInfo	NPKIT_x509IssuerAltNamesInfo
NWx509IssuerAltName	NPKIT_x509IssuerAltName
NWx509CRLDistributionPointsInfo	NPKIT_x509CRLDistributionPointsInfo
NWx509CRLDistributionPoint	NPKIT_x509CRLDistributionPoint
Not available	NPKIT_x509NovellExtensionInfo*
NWx509CreateContext	NPKIT_CRLCreateContext
NWx509FreeContext	NPKIT_CRLFreeContext

NWPKIAPI x509 Functions	NPKIT x509 Functions
NWx509DecodeCRL	NPKIT_CRLDecode
NWx509CRLEntryInfo	NPKIT_CRLEntryInfo
NWx509CRLExtensionInfo	NPKIT_CRLExtensionInfo
NWx509CRLEntryExtensionInfo	NPKIT_CRLEntryExtensionInfo
NWx509CRLReasonCodeInfo	NPKIT_CRLReasonCodeInfo
NWx509CRLInvalidityDateInfo	NPKIT_CRLInvalidityDateInfo
NWPKIVerifyCertificate	NPKIT_VerifyCertificate
NWPKIVerifyCertChain	NPKIT_VerifyCertChain
NWPKIVerifyCertChainWithCallback	NPKIT_VerifyCertChainWithCallback
NWPKIIssuerSubjectNameMatch	NPKIT_VerifyIssuerSubjectNameMatch
None	NPKIT_PKCS12CreateContext*[1]
None	NPKIT_PKCS12FreeContext*[1]
None	NPKIT_PKCS12Encode*[1]
None	NPKIT_PKCS12Decode*[1]
None	NPKIT_PKCS12ChainElement*[1]

2.2 Setting The Basic Constraints Field

The basic constraints field for NPKICreateOrganizationalCa, NPKICreateServerCertificate, NPKICreateUserCertificate, and NPKIGenerateCertificateFromCSR has been changed. The value field of the structure NPKI_Extension must be big endian. On Solaris and AIX, the flags used for basic constraints can just be assigned. On Windows, Netware, and Linux, they must be byte swapped, then assigned.

For more information on setting the basic constraints field, see the following:

- NPKI Basic Constraints Extension
- NPKIT Basic Constraints Extension Values

Certificate Server Error Code Constants

A

The Novell Certificate Server APIs use the error codes listed below:

Decimal Value	Hexidecimal Value	Name	Description
-1202	0xFFFFFB4E	PKI_E_FILE_OPEN	A file could not be opened.
-1201	0xFFFFFB4F	PKI_E_FILE_CREATE	A file could not be created.
-1203	0xFFFFFB4D	PKI_E_FILE_READ	A file could not be read.
-1204	0xFFFFFB4C	PKI_E_FILE_WRITE	A file could not be written.
-1205	0xFFFFFB4B	PKI_E_FILE_SEEK	The size of a file could not be determined.
-1206	0xFFFFFB4A	PKI_E_CRYPT_INIT	Not currently used.
-1207	0xFFFFFB49	PKI_E_NO_KEY_FILE	Not currently used.
-1208	0xFFFFFB48	PKI_E_GENERATE_KEY	Not currently used.
-1209	0xFFFFFB47	PKI_E_KEY_SIZE_NOT_SUPPORTED	The requested key size is not supported by NICI.
-1210	0xFFFFFB46	PKI_E_KEYS_ALREADY_EXIST	A key pair already exists for the Organizational CA.
-1211	0xFFFFFB45	PKI_E_UPDATE_KMO	A certificate with the specified key pair name already exists for the specified server.
-1212	0xFFFFFB44	PKI_E_INSUFFICIENT_MEMORY	Memory could not be allocated on either the client workstation or the server.
-1213	0xFFFFFB43	PKI_E_BUFFER_OVERFLOW	An internal data buffer overflow occurred.
-1214	0xFFFFFB42	PKI_E_BAD_REQUEST_SYNTAX	An invalid request was made to the client or server.
-1215	0xFFFFFB41	PKI_E_DSIO	Not currently used.
-1216	0xFFFFFB40	PKI_E_CREATE_CERTIFICATE_OR_CSR	The certificate or certificate signing request could not be generated.
-1217	0xFFFFFB3F	PKI_E_ALGORITHM_NOT_SUPPORTED	The requested key generation or signature algorithm is not allowed by NICI.

Decimal Value	Hexidecimal Value	Name	Description
-1218	0xFFFFFB3E	PKI_E_UNKNOWN_ATTRIBUTE	The requested subject name, issuer name, or alternative name contains a name type that is not understood by Novell Certificate Server.
-1219	0xFFFFFB3D	PKI_E_INVALID_NAME	A specified name is not valid for the requested operation.
-1220	0xFFFFFB3C	PKI_E_INVALID_CREATE_CA _REQUEST	Not currently used.
-1221	0xFFFFFB3B	PKI_E_INVALID_OBJECT	The specified object is not the expected type or does not contain the expected information.
-1222	0xFFFFFB3A	PKI_E_NOT_SUPPORTED	Novell Certificate Server does not support the requested operation.
-1223	0xFFFFFB39	PKI_E_ADD_TRUSTED_ROOT	Not currently used.
-1224	0xFFFFFB38	PKI_E_ADD_KEYPAIR	Not currently used.
-1225	0xFFFFFB37	PKI_E_ADD_CERTIFICATE	The User Certificate created was not stored in the User object.
-1226	0xFFFFFB36	PKI_E_EXPECTING_CERTIFICATE	An attempt was made to store a certificate or a certificate chain with an invalid encoding into a Server Certificate object.
-1227	0xFFFFFB35	PKI_E_BROKEN_CHAIN	The certificate chain being stored in a Server Certificate object is invalid or corrupted.
-1228	0xFFFFFB34	PKI_E_INIT_ERROR	The client could not initialize the required eDirectory context.
-1229	0xFFFFFB33	PKI_E_WRONG_VERSION	An unrecognized version of an NCP™ has been sent to the server. Data stored in the User object is not in a recognized format.
-1230	0xFFFFFB32	PKI_E_WRONG_PKI_E_ONLY_ONE_TREE_CA	An attempt was made to create an Organizational CA when one already exists. Only one Organizational CA is permitted in an eDirectory tree.

Decimal Value	Hexidecimal Value	Name	Description
-1231	0xFFFFFB31	PKI_E_BAD_ROOT_INDEX	The certificate chain stored in a Server Certificate objectServer_Certificate_Object has been corrupted. The certificate chain stored in the Organizational CA object has been corrupted.
-1232	0xFFFFFB30	PKI_E_SUBJECT_NAME_COMPARISON_FAILURE	The subject name stored in the Server Certificate object is not the same as the subject name within the certificate that is being stored. The subject name of a certificate in the Organizational CA's certificate chain does not match the expected value. The subject name of a certificate in the NICI Machine Unique CA's certificate chain does not match the expected value.
-1233	0xFFFFFB2F	PKI_E_PUBLIC_KEY_COMPARISON_FAILURE	The public key stored in the Server Certificate object is not the same as the public key within the certificate being stored.
-1234	0xFFFFFB2E	PKI_E_NO_RIGHTS	The user does not have the appropriate eDirectory rights to perform the operation.
-1235	0xFFFFFB2D	PKI_TERISA_ESTABLISH_CONTEXT_ERROR	The server could not establish a Terisa context.
-1236	0xFFFFFB2C	PKI_TERISA_ADD_ROOT_ERROR	The server could not add the specified certificate as a trusted root to the Server Certificate object.
-1237	0xFFFFFB2B	PKI_TERISA_ADD_KEYS_ERROR	The server could not store the public and private keys in the Server Certificate object.
-1238	0xFFFFFB2A	TERISA_ADD_CERTIFICATE _ERROR	The server could not store the specified certificate or certificate chain in the Server Certificate object.
-1239	0xFFFFFB29	PKI_E_SYSTEM_RESOURCES	The server could not allocate the required eDirectory context or the required NICI context.

Decimal Value	Hexidecimal Value	Name	Description
-1240	0xFFFFFB28	PKI_E_PARSE_CERTIFICATE	Novell Certificate Server was unable to parse a certificate that has been stored or is being stored.
-1241	0xFFFFFB27	PKI_E_NO_TREE_CA	An Organizational CA does not exist for the eDirectory tree.
-1242	0xFFFFFB26	PKI_E_INVALID_NICKNAME	A User Certificate with the specified nickname does not exist.
-1243	0xFFFFFB25	PKI_E_USER_ALREADY_IN_LIST	Not currently used.
-1244	0xFFFFFB24	PKI_E_USER_NOT_FOUND_IN_LIST	Not currently used.
-1246	0xFFFFFB22	PKI_E_USER_CERT_NOT_FOUND	Not currently used.
-1247	0xFFFFFB21	PKI_E_INVALID_ALGORITHM	The cryptographic algorithm is not supported.
-1248	0xFFFFFB20	PKI_E_INVALID_OPERATION	The requested operation cannot be performed by the Novell Certificate Server.
-1249	0xFFFFFB1F	PKI_E_INVALID_DIGEST	Not currently used.
-1251	0xFFFFFB1D	PKI_E_DATA_NOT_READY	The requested data is not available.
-1252	0xFFFFFB1C	PKI_E_INVALID_KDK_ID	Not currently used.
-1253	0xFFFFFB1B	PKI_E_INTERNAL_ERROR	An unexpected internal error has occurred.
-1254	0xFFFFFB1A	PKI_E_INVALID_CERTIFICATE_TIME	The validity period requested for the certificate is not valid. The Organizational CA is not yet operational.
-1255	0xFFFFFB19	PKI_E_EXPIRED_CERTIFICATE	A certificate is no longer valid because it has expired.
-1256	0xFFFFFB18	PKI E INVALID SIGNATURE	Not currently used.
-1257	0xFFFFFB17	PKI_E_KDK_TABLE_FULL	Not currently used.
-1258	0xFFFFFB16	PKI_E_CERT_INVALID	The certificate is invalid.
-1259	0xFFFFFB15	PKI_E_CA_ALREADY_INSTALLED	Not currently used.
-1260	0xFFFFFB14	PKI_E_CA_NOT_OPERATIONAL	The specified server is not a CA. The server specified is not running the Novell Certificate Server.

Decimal Value	Hexidecimal Value	Name	Description
-1261	0xFFFFFB13	PKI_E_KEY_FAILURE	An error occurred while transporting a private key to the client.
-1262	0xFFFFFB12	PKI_E_INVALID_KEY_ID	The specified certificate nickname could not be found.
-1263	0xFFFFFB11	PKI_E_ACCESS_DENIED	The user does not have the appropriate eDirectory rights to perform the operation.
-1264	0xFFFFFB10	PKI_E_NICI_OUT_OF_SYNC	An NICI session error occurred while attempting to transfer a private key.
-1265	0xFFFFFB0F	PKI_E_NO_SECURITY_CONTAINER	The Security container cannot be found.
-1266	0xFFFFFB0E	PKI_E_NO_IP_ADDRESSES	No IP address can be found for the specified server.
-1267	0xFFFFFB0D	PKI_E_NICKNAME_IN_USE	The nickname specified is already being used.
-1268	0xFFFFFB0C	PKI_E_NOT_CONNECTED_TO_SERVICE	You are not currently connected to a server which can perform the requested operation.
-1269	0xFFFFFB0B	PKI_E_DUPLICATE	Not currently used.
-1270	0xFFFFFB0A	PKI_E_CRL_INVALID	The CRL is invalid.
-1271	0xFFFFFB09	PKI_E_CERT_NOT_FOUND	The specified certificate could not be found.
-1272	0xFFFFFB08	PKI_E_INVALID_CONTEXT	The specified context is not currently valid.
-1273	0xFFFFFB07	PKI_E_SERVICE_NOT_AVAILABLE	***The specified service is not available.

Revision History

B

Revision Date	Changes
October 11, 2006	Updated source code to the 3.2.0 version.
March 1, 2006	• Relocated summary listing of the Certificate Server APIs from the Overview to Getting Started section to fix link problems. • Fixed broken links.
October 5, 2005	• Transitioned to revised Novell documentation standards.
March 2, 2005	Revised document to conform with requirements of Novell Forge.
October 6, 2004	• Made technical corrections and fixed broken links.
June 9, 2004	• Rolled in the latest version of the 2.72.1 code, which includes all bug fixes for future releases • Made minor documentation updates.
February 18, 2004	Made minor edits to fix broken links.
October 8, 2003	• Changed name from Certificate Server Libraries to Certificate Server Libraries for C. • Updated product registration and trademark information.
March 2003	• Added Chapter 2, “Updating Certificate Server APIs,” on page 13 to explain how to convert the original Certificate Server API (PKIS) to the new functionality provided by NPKI and NPKIT. • Updated links to NPKI sample code.
January 2003	Expanded this library with the addition of new NDK: Novell Public Key Infrastructure Toolbox (NPKIT) and NDK: Novell Certificate Server Library for C Version 2 (NPKI) APIs. NPKIT is a cross platform (all platforms supported by eDirectory™ 8.7) public key utility library. NPKI is a cross platform (all platforms supported by eDirectory 8.7) public key management library that does not depend on a Novell® client. Both of these APIs are required to replace the functionality of Certificate Server Library for C Version 1(NWPKI) (http://forge.novell.com/modules/xfcontent/private.php/ncslibv1/README.html).

Glossary

This section defines a number of terms that are used in the Certificate Server Libraries document.

AIX
Advanced Interactive Executive

An IBM version of the UNIX operating system.

CA
Certificate Authority

An entity that issues the digital certificates used in public-key cryptography and attests to the identity of the person or organization to whom it issues the digital certificates. It also is called certification authority or certifying authority.

PKI
Public Key Infrastructure

The PKI framework used to securely exchange information, using certification authorities (CAs) and digital signatures to verify and authenticate the validity of persons engaged in Internet, intranet, and extranet transactions. A reliable PKI system is necessary before implementing a secure e-commerce strategy.

KMO
Key Material Object

The PKI framework used to securely exchange information, using certification authorities (CAs) and digital signatures to verify and authenticate the validity of persons engaged in Internet, Intranet, and Extranet transactions. A reliable PKI system is necessary before implementing a secure e-commerce strategy.

X.509 Certificates
X.509 certificates are the current industry standard for digital certificates. However, companies have implemented the X.509 standard in different ways, rendering some generated X.509 Certificates unreadable across software products from different companies. See X.509 Property Page (http://www.novell.com/documentation/lg/nw5/docui/index.html#../ussecur/crndsenu/data/h0000070.html) for digital certificate specifications that have been recommended by the International Telecommunications Union (ITU) since 1988.