

Novell Developer Kit

www.novell.com

October 17, 2007

NOVELL CERTIFICATE SERVER™
CLASSES FOR JAVA*



Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to [Novell International Trade Services \(http://www.novell.com/info/exports\)](http://www.novell.com/info/exports) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 1993-2006 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.novell.com/company/legal/patents/> and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell developer products, and to get updates, see developer.novell.com/ndk. To access online documentation for Novell products, see www.novell.com/documentation.

Novell Trademarks

For a list of Novell trademarks, see [Trademarks \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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	7
1 Concepts	9
1.1 Dependencies	9
2 JavaDoc API Reference	11
A Revision History	13

About This Guide

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

JPKI will help you use this functionality to further enhance or customize your security solutions without re-writing your own technology.

For more information about the Novell implementation of Certificate Server, see *NDK: Novell Certificate Server APIs - Overview*.

This guide contains the following sections:

- ♦ Chapter 1, “Concepts,” on page 9
- ♦ Chapter 2, “JavaDoc API Reference,” on page 11

Audience

This guide is intended for Certificate Server developers familiar with the Java programming language.

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 Classes for Java \(http://developer.novell.com/wiki/index.php/Novell_Certificate_Server_Classes_for_Java\)](http://developer.novell.com/wiki/index.php/Novell_Certificate_Server_Classes_for_Java).

Additional Documentation

For more comprehensive background information about setting up, managing, and troubleshooting this service, see the [Novell Certificate Server Administration Guide \(http://www.novell.com/documentation/crt311/index.html\)](http://www.novell.com/documentation/crt311/index.html).

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

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

For help with Certificate Server problems or questions, visit the [Novell NCSLIB Support Forum \(http://forge.novell.com/modules/xfmod/newsportal/thread.php?group_id=1258&group=novell.devsup.ncsjava\)](http://forge.novell.com/modules/xfmod/newsportal/thread.php?group_id=1258&group=novell.devsup.ncsjava).

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.

The Novell® Certificate Server Classes for Java (JPKI) map all functionality of the Novell Certificate Server C APIs. In other words, anything that can be done in the C APIs can also be done in the Java API. JPKI closely resembles the C API so the learning curve of those using the C functions should be short.

For more information about the Novell Certificate Server C APIs, see *NDK: Novell Certificate Server Library for C Version 2* and *NDK: Novell Public Key Infrastructure Toolbox*. To understand conceptual about the implementation of Novell Certificate Server, see *NDK: Novell Certificate Server APIs - Overview*.

1.1 Dependencies

JPKI depends on the C API native code, specifically PKIAPI and NPKIT. It therefore has the same dependencies as those libraries. The Java API is contained in npki.jar, which contains the JNI interface for both PKIAPI and NPKIT. It also contains helper classes that are used to pass parameters to the API and receive return values. Errors are thrown from calls to the API.

JPKI contains functions that enable you to manage and access certificates. NPKI methods require an authentication to eDirectory™, while the NPKIT methods are directory independent. A suggested implementation is to extend the NPKIAPI object and provide the connection information suited to your particular needs.

The new version of the PKI code (3.1x) will run on eDirectory, however new features are only supported in eDirectory 8.8.x and above (that is, although the features may work on eDirectory 8.7x, they have only been tested and are officially supported only on eDirectory 8.8x and above).

The new features, which are only supported on eDirectory 8.8, consist of the following:

- ♦ Certificate Server creation of CRL distribution points:
 - ♦ Functionality that creates and uses PKI Container object(s).
 - ♦ Functionality that creates and uses CRL Configuration object(s).
 - ♦ Functionality that creates and uses CRL Distribution Point object(s).
 - ♦ Issuing CRLs.
 - ♦ Revocation of certificates.
- ♦ Support for Subordinate CAs; that is, having the Organizational CA be subordinate to either a third-party CA or another eDirectory tree.
- ♦ Support for 4096 bit key size; that is, support for key-sizes greater than 2048 bits.

Click to open the on-line [JavaDoc API Reference and NPKIAPI_SAMPLE.java documentation \(http://developer.novell.com/ndk/doc/ncsjava/jpki_enu/api/index.html\)](http://developer.novell.com/ndk/doc/ncsjava/jpki_enu/api/index.html) for the following Novell Certificate Server Java classes:

- ♦ [NPKI_AccessDescription \(../api/com/novell/security/japi/pki/NPKI_AccessDescription.html\)](#)
- ♦ [NPKI_AltName \(../api/com/novell/security/japi/pki/NPKI_AltName.html\)](#)
- ♦ [NPKI_ASN1_Extensions \(../api/com/novell/security/japi/pki/NPKI_ASN1_Extensions.html\)](#)
- ♦ [NPKI_CertChain \(../api/com/novell/security/japi/pki/NPKI_CertChain.html\)](#)
- ♦ [NPKI_Certificate \(../api/com/novell/security/japi/pki/NPKI_Certificate.html\)](#)
- ♦ [NPKI_CertificateName \(../api/com/novell/security/japi/pki/NPKI_CertificateName.html\)](#)
- ♦ [NPKI_CertificateNamesList \(../api/com/novell/security/japi/pki/NPKI_CertificateNamesList.html\)](#)
- ♦ [NPKI_crl \(../api/com/novell/security/japi/pki/NPKI_crl.html\)](#)
- ♦ [NPKI_crlCacheContext \(../api/com/novell/security/japi/pki/NPKI_crlCacheContext.html\)](#)
- ♦ [NPKI_crlList \(../api/com/novell/security/japi/pki/NPKI_crlList.html\)](#)
- ♦ [NPKI_Error \(../api/com/novell/security/japi/pki/NPKI_Error.html\)](#)
- ♦ [NPKI_ErrorList \(../api/com/novell/security/japi/pki/NPKI_ErrorList.html\)](#)
- ♦ [NPKI_Exception \(../api/com/novell/security/japi/pki/NPKI_Exception.html\)](#)
- ♦ [NPKI_ExtAIAValues \(../api/com/novell/security/japi/pki/NPKI_ExtAIAValues.html\)](#)
- ♦ [NPKI_ExtAltNames \(../api/com/novell/security/japi/pki/NPKI_ExtAltNames.html\)](#)
- ♦ [NPKI_Extension \(../api/com/novell/security/japi/pki/NPKI_Extension.html\)](#)
- ♦ [NPKIAPI \(../api/com/novell/security/japi/pki/NPKIAPI.html\)](#)
- ♦ [NPKITcache \(../api/com/novell/security/japi/pki/NPKITcache.html\)](#)
- ♦ [NPKITcertificate \(../api/com/novell/security/japi/pki/NPKITcertificate.html\)](#)
- ♦ [NPKITcrl \(../api/com/novell/security/japi/pki/NPKITcrl.html\)](#)
- ♦ [NPKITcsr \(../api/com/novell/security/japi/pki/NPKITcsr.html\)](#)
- ♦ [NPKITtoolbox \(../api/com/novell/security/japi/pki/NPKITtoolbox.html\)](#)
- ♦ [NPKITverify \(../api/com/novell/security/japi/pki/NPKITverify.html\)](#)
- ♦ [NPKITx509 \(../api/com/novell/security/japi/pki/NPKITx509.html\)](#)
- ♦ [NPKITx509CertList \(../api/com/novell/security/japi/pki/NPKITx509CertList.html\)](#)
- ♦ [OSUtil \(../api/com/novell/security/japi/pki/OSUtil.html\)](#)

Revision History



Revision Date	Changes
October 17, 2007	<ul style="list-style-type: none">♦ Updated source code to version 3.3.0. New features include:<ul style="list-style-type: none">♦ Added support for the SHA-2 signing algorithm.♦ Added support for forcing the acquisition of a new CRL rather than using a cached CRL during certificate chain validation.♦ Added support for User and Server Self-Provisioning via the new SecurityRightsLevel APIs.♦ Added the capability to require Write rights to operate the CA via the new SecurityRightsLevel APIs.♦ Added the capability to allow any authenticated user to cause the CA to issue an emergency CRL via the new SecurityRightsLevel APIs.♦ Added support for the PKCS#8 Private Key type in the NPKIT PEM types.♦ Made changes to support 64 bit versions.♦ Added a flag for NPKITGetServerInfo that is used to remotely start the Server Health Check.♦ Added a flag for NPKITCreateDefaultCertificates which will cause the default certificates to be re-created if the CA has changed♦ Changed NPKITCreateDefaultCertificates to automatically add subject alternative names when creating the default certificates.♦ Added APIs to configure the new KMO Export functionality which can export a KMO's certificates and private-key to the file system in a format consistent with Apache or OpenSSL Servers. (This functionality is not needed or available on NetWare.)♦ Various bug fixes.
October 11, 2006	<ul style="list-style-type: none">♦ Changed component from Early Access to Novell Supported status.♦ Updated source code to version 3.2.0.
June 21, 2006	<ul style="list-style-type: none">♦ Enhance identification and accessibility of Java classes from the documentation.♦ Added the Version 3.2 Java code for supported PEM types in NPKITcache and options for flags in NPKITverify.♦ Fixed broken Java links.
March 1, 2006	<ul style="list-style-type: none">♦ Updated Javadoc for 3.1.1 code release.♦ Updated Section 1.1, "Dependencies," on page 9.♦ Fixed broken links.
October 5, 2005	<ul style="list-style-type: none">♦ Transitioned to revised Novell documentation standards.
March 5, 2005	<ul style="list-style-type: none">♦ Updated document to comply with requirements of Novell Forge.♦ Fixed broken links.

Revision Date	Changes
October 6, 2004	<ul style="list-style-type: none"> ◆ Made technical corrections and fixed broken links.
June 9, 2004	<ul style="list-style-type: none"> ◆ 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	<ol style="list-style-type: none"> 1. Made minor editorial revisions and updated broken links to Novell Certificate Server Libraries for C (http://developer.novell.com/ndk/ssocomp.htm). 2. Revised Javadoc version to PKI_2.52. 2. As part of version PKI_2.52 revisions, added the following Java classes to the API (see the JavaDoc API Reference and NPKI_API_SAMPLE.java documentation (http://developer.novell.com/ndk/doc/ncsjava/jpki_enu/api/index.html)): <ul style="list-style-type: none"> NPKIT_cache NPKI_CertificateName NPKI_CertificateNamesList NPKI_Error NPKI_ErrorList
October 8, 2003	<ul style="list-style-type: none"> ◆ Changed name from Certificate Server Java API to Novell Certificate Server Classes for Java. ◆ Updated product registration and trademark information.
June 2003	Add Certificate Server Java API as a new NDK component.