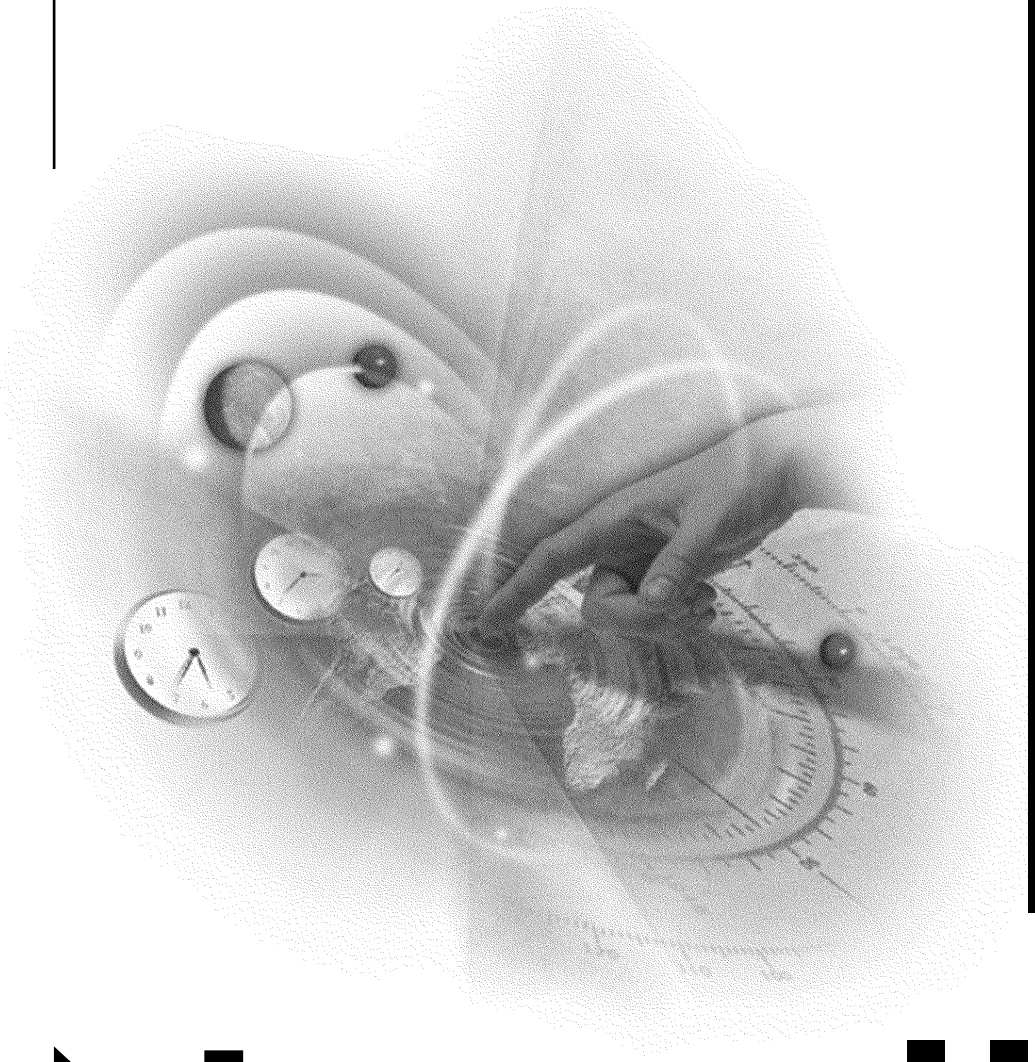
VERSION 2.0

Novell Certificate Server

PUBLIC KEY CRYPTOGRAPHY SERVICES

Administration Guide



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.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

U.S. Patent Nos. 5,870,739, 5,873,079; and 5884,304. U.S. and Foreign Patents Pending.

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

www.novell.com

Novell Certificate Server Administration Guide
October 1999
104-001170-001

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

Novell Trademarks

ConsoleOne is a trademark of Novell, Inc.

GroupWise is a registered trademark of Novell, Inc., in the United States and other countries.

NetWare is a registered trademark of Novell, Inc., in the United States and other countries.

Novell is a registered trademark of Novell, Inc., in the United States and other countries.

Novell Authorized Reseller is a service mark of Novell, Inc.

Novell Client is a trademark of Novell, Inc.

Novell Directory Services and NDS are registered trademarks of Novell, Inc., in the United States and other countries.

ZENworks is a trademark of Novell, Inc.

Third-Party Trademarks

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

Contents

Novell Certificate Server Administration Guide

Novell® Certificate Server provides public key cryptography services that are natively integrated into Novell Directory Services® (NDS®) services and that allow you to mint, issue, and manage both user and server certificates. These services allow you to protect confidential data transmissions over public communications channels such as the Internet.

This book describes the functionality of Novell Certificate Server, how to set it up, and how to manage it. This book also provides some basic information about how public key cryptography works.

1 Overview

Novell® Certificate Server provides public key cryptography services that are natively integrated into Novell Directory Services® (NDS®) and that allow you to mint, issue, and manage both user and server certificates. These services allow you to protect confidential data transmissions over public communications channels such as the Internet.

NOTE: If you are unfamiliar with public key cryptography concepts, see "Public Key Cryptography Basics" on page 53.

Public key cryptography presents unique challenges to network administrators. Novell Certificate Server helps you meet these challenges in the following ways:

- **Provides public key cryptography services on your network**

  You can create an Organizational Certificate Authority (CA) within your NDS 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 key pairs, and issue public key certificates through the Organizational CA.

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

  Key pairs are stored in NDS and can therefore leverage NDS 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 Crytography 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 NDS, and backed up using standard NDS backup utilities.

- **Allows central administration of certificates using ConsoleOne™**

  A ConsoleOne snapin allows you to manage certificates issued from either a Novell CA or from the Entrust* CA product.

- **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 system administrator intervention.

- **Supports popular e-mail clients and browsers**

  Novell Certificate Server allows you to create and manage user certificates for securing e-mail. Novell Certificate Server supports GroupWise® 5.5, Microsoft* Outlook98 and Outlook2000, Netscape* Messenger*, and other popular e-mail clients. It's also compatible with both Netscape Navigator* and Microsoft Internet Explorer.

IMPORTANT: The cryptography services available in this product depend on the country in which your network is located. Novell Certificate Server will not function if cryptography services are not fully installed. For example, the mass-market exportable version of NICI is limited to 512-bit RSA keys for data encryption. The U.S. and Canadian version of NICI supports key sizes up to 2,048 bits for all types of keys.

To ensure that you have the highest level of cryptography services available in your area, contact your Novell Authorized Reseller℠.

Product Components

Novell Certificate Server

Novell Certificate Server consists of the PKI NLM (NetWare) and a snap-in module to ConsoleOne, which is the administration point for Novell Certificate Server. Novell Certificate Server allows you to request, manage, and store public key certificates and their associated key pairs in the NDS tree, and to establish an Organizational certificate authority that is specific to your NDS tree and your organization.

Novell Certificate Server derives all supported cryptography and signature algorithms, as well as supported key sizes, from Novell International Cryptographic Infrastructure (NICI). Therefore, a single version of Novell Certificate Server can be used in installations throughout the world.

After installing Novell Certificate Server, you will manage it using ConsoleOne running on a client. (Novell Certificate Server cannot be managed using ConsoleOne running on a NetWare server console.)

Through ConsoleOne, you can perform the following tasks:

- **Create an Organizational certificate authority for your organization**

  During the installation, you can elect to create an Organizational Certificate Authority (CA) if one does not already exist in the NDS tree. Using ConsoleOne, you may also create or recreate the Organizational CA after the installation is completed.

  The Organizational CA object contains the public key, private key, certificate, certificate chain, and other configuration information for the Organizational CA. The Organizational CA object resides in the Security container in NDS.

  Once a server is configured to provide the certificate authority service, it performs that service for the entire NDS tree.

- **Create a Server Certificate object for each cryptography-enabled application**

  During the installation, you can elect to create a Server Certificate object. You may create other Server Certificate objects after the installation is completed.

  The Server Certificate object contains the public key, private key, certificate, and certificate chain that enables SSL security services for server applications.

  A server can have many Server Certificate objects associated with it. Any cryptography-enabled applications running on a particular server can be configured to use any one of the Server Certificate objects for that server. Multiple applications running on a given server can use the same Server Certificate object; however, a Server Certificate object cannot be shared between servers.

  You can create Server Certificate objects only in the container where the server resides. If the Server object is moved, all Server Certificate objects belonging to that server must be moved as well. You should not rename a Server Certificate object. You can determine which Server Certificate objects belong to a server by searching for the server's name in the Server Certificate Object Name.

  NOTE: The key pair stored in the Server Certificate object is referenced by the name you enter when the key pair is created. The key pair name is not the name of the Server Certificate object. When configuring cryptography-enabled applications to use key pairs, you reference those keys by their key pair name, not by the Server Certificate object name.

- **Request public key certificates from the Organizational certificate authority or from an external certificate authority.**

  A public key certificate contains a public key, a name, and a signature. The signature is created by the CA, and provides a cryptographic binding between the public key and a name.

  Public key certificates contain, at minimum, a public key, a subject name, an issuer name, a validity period, a serial number, and a certificate authority-generated signature. They may also contain specific extensions—for example, to further clarify the use of the certificate.

- **Create a user certificate**

  A user certificate is intended to allow users to send and receive digitally signed and encrypted e-mail using the S/MIME standard. Users have access to their own user certificates and private keys, which can be used for authentication, data encryption/decryption, digital signing, and secure e-mail.

  Generally, only the CA administrator has sufficient rights to create user certificates. However, only the user has rights to export or download the private key from NDS. Any user can export any other user's public key certificate.

  The user certificate is created from the Security tab of the user's property page and are signed by the Organizational CA.

  Multiple certificates can be stored on the user's object.

- **Create a Trusted Root Container**

  A trusted root provides the basis for trust in public key cryptography. Trust roots are used to validate certificates signed by the CA. Trusted roots enable security for SSL, secure e-mail, and certificate-based authentication.

  A Trusted Root Container is an NDS object that contains Trusted Root objects.

  You must create the Trusted Root Container in the Security Container.

- **Create a Trusted Root object**

  A Trusted Root object is an NDS object that contains a CA's Trusted Root certificate that is known to be authentic and valid. The Trusted Root Certificate can be exported and used as needed. Applications that are configured to use the Trusted Root Certificate will consider a certificate valid if it has been signed by one of the CAs in the Trusted Root Container.

  The Trusted Root object must reside in a Trusted Root Container.

Novell International Cryptographic Infrastructure

Novell International Cryptographic Infrastructure (NICI) is the underlying cryptographic infrastructure that provides the cryptography for Novell Certificate Server, Novell Authentication Service, and other applications.

NICI must be installed on the server in order for Novell Certificate Server to work properly. NICI ships with Novell Certificate Server, and you install NICI using a manual process described in the Installation quick start. When Novell Certificate Server ships with other products, you may be required to install NICI manually, or NICI may be automatically installed. Refer to the product's installation guide for more information.

Novell Certificate Console

Novell Certificate Console is a user-oriented utility that can export a user's certificate and private key without having ConsoleOne running on the workstation. Novell Certificate Console is a convenient way to give user's access to their user certificates and keys without needing to give them access to ConsoleOne.

The Novell Certificate Console interface is very similar to the User Certificate property page in ConsoleOne and provides the same user certificate export functionality.

See "Exporting a User Certificate Using Novell Certificate Console" on page 39 for instructions on setting up this utility.

For Additional Information

For instructions on installing Novell Certificate Server as a stand-alone product, see the installation quick start card, which is included in the software download as CERTSERV_INSTALL.PDF.

For instructions on installing Novell Certificate Server when it is included with another Novell product, see the installation guide for that product.

For instructions on setting up Novell Certificate Server, see "Setting Up Novell Certificate Server" on page 17.

For information about administering Novell Certificate Server, see “Managing Novell Certificate Server” on page 25.

For information about setting up Novell Certificate Console, see “Exporting a User Certificate Using Novell Certificate Console” on page 39

For the latest online documentation for this and other Novell products, see the Product Documentation Web site (http://www.novell.com/documentation/).

For additional information about this and other Novell security products and technologies, see the following Web sites:

http://www.novell.com/security (http://www.novell.com/security)

http://www.novell.com/products/cryptography/ (http://www.novell.com/products/cryptography/)

2 Setting Up Novell Certificate Server

After you install Novell® Certificate Server, you must set it up for use on your network by completing the following tasks:

- “Deciding Which Type of Certificate Authority to Use” on page 17
- “Creating an Organizational Certificate Authority Object” on page 19
- “Creating Server Certificate Objects” on page 20 for applications whose secure transmissions you want to manage.
- “Configuring Cryptography-Enabled Applications” on page 22

Deciding Which Type of Certificate Authority to Use

You can manage public key certificates, Server Certificate objects, and their associated components and sign the public key certificates using either an Organizational Certificate Authority or an external Certificate Authority. During the Server Certificate object creation process, you will be asked which type of Certificate Authority will sign the Server Certificate object.

The Organizational Certificate Authority is specific to your organization and uses an organizational-specific public key for signing operations. The private key is created when you create the Organizational Certificate Authority.

An external Certificate Authority is managed by a third party outside of the NDS tree. An example of an external Certificate Authority is VeriSign*.

Novell Certificate Server allows you to create certificates for both servers and end users. Server Certificates can be signed by either the Organizational CA or by an external or third-party CA. User certificates can be signed by only the Organizational CA for this release only.

Both types of Certificate Authorities can be used simultaneously. Using one type of Certificate Authority does not preclude the use of the other.

Benefits of Using an Organizational Certificate Authority Provided with Novell Certificate Server

- **Compatibility.** An Organizational Certificate Authority is compatible with other applications that share a common trusted root in NDS®. These include BorderManager™, LDAP Services, and future products using Novell security.

- **Cost savings.** An Organizational Certificate Authority lets you create an unlimited number of public key certificates at no cost; obtaining a single public key certificate through an external Certificate Authority might cost hundreds of dollars.

- **Component of a complete and compatible solution.** By using the Organizational Certificate Authority, you can use the complete cryptographic system build into NDS without having to rely on any external services. In addition, Novell Certificate Server is compatible with a wide range of Novell products.

- **Certificate attribute and content control.** An Organizational Certificate Authority is managed by the network administrator, who decides upon public key certificate attributes such as certificate life span, key size, and signature algorithm.

- **Simplified management.** The Organizational Certificate Authority performs a function similar to external certificate authorities but without the added cost and complexity.

Benefits of Using an External Certificate Authority

- **Liability.** An external Certificate Authority might offer some liability protection if, through the fault of the Certificate Authority, your private key was exposed or your public key certificate was misrepresented.

- **Availability.** An external Certificate Authority may be more widely available and compatible with applications outside of NDS.

Creating an Organizational Certificate Authority Object

The Novell Certificate Server installation process, by default, will create the Organizational Certificate Authority (CA) for you. You will be prompted to specify an Organizational CA name. When you click Finish, the Organizational CA will be created with the default parameters and placed in the Security container.

If you desire more control over the creation of the Organizational CA, you can create the Organizational CA manually. Also, if you delete the Organizational CA, you will need to follow this procedure to recreate it.

To create the Organizational Certificate Authority object:

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see “Creating an Organizational CA” on page 59.

2. Start ConsoleOne™.

3. Expand the NDS tree in which you would like to create the Organizational Certificate Authority.

   This reveals the Security container object.

4. Right-click the Security container object and select New > Object.

5 From the list box in the New Object dialog box, double-click NDSPKI:Certificate Authority.

This opens the Create an Organizational Certificate Authority Object dialog box and the corresponding wizard that creates the object. For specific information on the dialog box or any of the wizard pages, click Help.

NOTE: You can have only one Organizational CA for your NDS Tree.

IMPORTANT: During the creation process, you will be prompted to name the Organizational Certificate Authority object and to choose a server on which the Certificate Authority service will run.

Select a server that is physically secure, that will be available when needed to perform signing operations, that runs a protocol that is compatible with the other servers in your organization (for example, IP, IPX™, IP/IPX), and that only runs software that you trust. It is important that your server meet these conditions, because the Organizational Certificate Authority object is the centerpiece of your PKI system and if the server that contains the object is compromised, your entire PKI system could be compromised as well.

Creating Server Certificate Objects

Server Certificate objects are created in the container that holds the server's NDS object. Depending on your needs, you may create a separate Server Certificate object for each cryptography-enabled application on the server. Or you may create one Server Certificate object for all applications used on that server.

NOTE: The terms Server Certificate Object and Key Material Object are synonymous. The schema name of the NDS object is NDSPKI:Key Material.

The Novell Certificate Server installation process can create a Server Certificate object for you. You will be prompted to specify a Server Certificate object name. When you click Finish, the Server Certificate object will be created with the default parameters and placed in the container where the target server resides.

If you want more control over the creation of the Server Certificate object, you can create the Server Certificate object manually, or you can use this procedure to create additional Server Certificate objects.

To create additional Server Certificate objects:

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Creating Server Certificate Objects" on page 60.

2. Start ConsoleOne.

3. Right-click the container object that contains the server that will run your cryptography-enabled applications; then select New > Object.

4. From the list box in the New Objects dialog box, double-click NDSPKI:Key Material.

   This opens the Create a Server Certificate dialog box and the corresponding wizard that creates the Server Certificate object. For specific information on the dialog box or any of the wizard pages, click Help.

Hints for Creating Server Certificates

During the Server Certificate object creation process, you will be prompted to name the key pair and choose the server that the key pair will be associated with. The Server Certificate object is generated by Novell Certificate Server, and its name is based on the key pair name that you choose.

If you choose the Custom creation method, you will also be prompted to specify whether the Server Certificate object will be signed by your organization's Organizational Certificate Authority or by an external Certificate Authority. For information about making this decision, see "Deciding Which Type of Certificate Authority to Use" on page 17.

If you decide to use your organization's Organizational CA, the server that the Server Certificate object is associated with must be able to communicate with the server that hosts the Organizational CA, or it must be the same server. These servers must be running the same protocol (IP/IPX).

If you decide to use an external Certificate Authority to sign the certificate, the server that the Server Certificate object is associated with will generate a certificate signing request that you will need to submit to the external Certificate Authority. After the certificate is signed and returned to you, you will need to install it into the Server Certificate object, along with the trusted root for the external Certificate Authority. For specific information on any of the wizard pages, click Help.

Once you have created the Server Certificate object, you can configure your applications to use them. (See "Configuring Cryptography-Enabled Applications" on page 22.) Keys are referenced in the application's configuration by the key pair name that you entered when you created the Server Certificate object.

Configuring Cryptography-Enabled Applications

Once you have configured Novell Certificate Server, you must configure your individual cryptography-enabled applications so that they can use the Novell certificates that you created. The configuration procedures will be unique to the individual applications, so we recommend that you consult the application's documentation for specific instructions.

See "Application Tasks" on page 45 for specific instructions on configuring GroupWise 5.5, Outlook98, Outlook2000, and Netscape* Messenger*

Additional Components to Set Up

Novell Certificate Server includes some additional components that can be set up to provide additional functionality.

Creating User Certificates

To create user certificates

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Creating User Certificates" on page 60.

2. Start ConsoleOne.

3 Double-click the User object that will host the user certificate.

4 Click Create.

This opens a wizard that helps you create the user certificate. For specific information on the wizard pages, click Help.

Creating a Trusted Root Container

You must create all Trusted Root Containers in the Security container.

To create a Trusted Root Container:

1 Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see “Creating a Trusted Root Container” on page 61.

2 Start ConsoleOne.

3 Right-click the container you want to create the Trusted Root Container in and click New > Object.

4 From the list box in the New Object dialog box, double-click NDSPKI:Trusted Root.

This opens the New NDSPKI:Trusted Root wizard that helps you create the trusted root container. For specific information on the wizard pages, click Help.

Creating Trusted Root Objects

A Trusted Root object can only reside in a Trusted Root Container.

To create Trusted Root objects:

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see “Creating Trusted Root Objects” on page 61.
2. Start ConsoleOne.
3. Open the Security container.
4. Right-click the Trusted Root Container object and click New > Object.
5. From the list box in the New Object dialog box, double-click NDSPKI:Trusted Root Object.

   This opens the Create a Trusted Root Object wizard that helps you create the trusted root object. For specific information on the wizard pages, click Help.

3 Managing Novell Certificate Server

As a system administrator, you will need to perform several tasks to maintain the public key cryptography services provided through Novell® Certificate Server. Most of these tasks are performed within ConsoleOne™. Some tasks are performed using the Novell Certificate Console utility. This chapter provides a brief overview and specific information on completing each task. p.

Certificate Authority Tasks:

Server Certificate Object Tasks:

- “Deleting a Server Certificate Object” on page 34
- “Viewing a Server Certificate Object’s Properties” on page 35
- “Viewing a Server Certificate Object’s Public Key Certificate Properties” on page 35
- “Viewing a Server Certificate Object’s Trusted Root Certificate Properties” on page 36

User Certificate Tasks:

- “Creating User Certificates” on page 22
- “Viewing a User Certificate’s Properties” on page 37
- “Exporting a User Certificate Using ConsoleOne” on page 38
- “Exporting a User Certificate Using Novell Certificate Console” on page 39

Trusted Root Object Tasks:

- “Creating a Trusted Root Container” on page 23
- “Creating Trusted Root Objects” on page 24
- “Viewing a Trusted Root Object’s Properties” on page 40
- “Replacing a Trusted Root Certificate” on page 41

NDS® Tasks:

- “Merging Two Trees that Have Security Containers” on page 42
- “Resolving Multiple Security Containers, Organizational CAs, KAP Containers, and W0 Objects” on page 43
- “Restoring or Re-creating a Security Container” on page 44
- “Restoring or Re-creating KAP and W0” on page 44

Application Tasks:

- “Exporting the Organizational CA’s Self-Signed Certificate and User Certificate” on page 45
- “Importing the Organizational CA’s Self-Signed Certificate into Your Internet Browser” on page 46
- “Importing the User Certificate into Your E-mail Client” on page 48
- “Configuring Your E-mail Client to Secure Your E-mail” on page 50

Certificate Authority Tasks

Creating an Organizational Certificate Authority Object

This task was discussed in Chapter 2. See “Creating an Organizational Certificate Authority Object” on page 19.

Issuing a Public Key Certificate

This task allows you to generate certificates for cryptography-enabled applications that do not recognize Server Certificate objects.

Your Organizational CA works the same way as an external CA, in that it has the ability to issue certificates from Certificate Signing Requests (CSRs). You can issue certificates using your Organizational CA when a user sends a CSR to you for signing. The user requesting the certificate can then take the issued certificate and import it directly into the cryptography-enabled application.

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see “Issuing a Public Key Certificate” on page 59.
2. Start ConsoleOne.
3. Click a Container object.
4. On the menu bar, select Tools > Issue Certificate.

5. Paste a Certificate Signing Request (CSR) into the dialog box, or use the browse button to locate a CSR file and open it in the dialog box.

6. Click Next.

7. Select the Certificate Authority (CA) that will sign the certificate, then click Next.

   NOTE: You can select the Organizational CA or, if your installation of Novell Certificate Server supports it, another NDS CA.

8. Specify how the key is to be used, then click Next.

9. Specify the subject name, the validity period, and the effective and expiration dates, then click Next.

10. Review the parameters sheet. If it is correct, click Finish. If not, click Back until you reach the point where you need to make changes.

    When you click Finish, a dialog box explains that a certificate has been created. You can save the certificate to the system clipboard in base64 format, to a base64-formatted file, or to a binary DER-formatted file. You can also click Details to view details about the issued certificate.

Viewing the Organizational CA's Properties

ConsoleOne allows you to view the Organizational CA's properties. Besides the NDS rights and properties that are viewable with any NDS object, you can also view properties specific to the Organizational CA, including the properties of the public key certificate and the self-signed certificate associated with it.

These properties provide you with the information that you need to perform any task related to this object.

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Viewing the Organizational CA's Properties and Certificates" on page 59.

2. Start ConsoleOne.

3 Double-click the Organizational CA object.

This brings up the property pages for the Organizational CA, which include a General page, a Certificates page, and property pages related to NDS.

4 Click the tabs that you wish to view.

Viewing an Organizational CA's Public Key Certificate Properties

1 Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Viewing the Organizational CA's Properties and Certificates" on page 59.

2 Start ConsoleOne.

3 Double-click the Organizational Certificate Authority object.

4 Click the Certificates tab.

5 Click the down-arrow to see the certificates available to view.

6 Click the Public Key Certificate.

This property page displays the fully-typed name of the subject, the issuer's fully-typed name, and the validity dates of the public key certificate.

7 To view additional information about an installed public key certificate, click Details.

The Details page displays information contained in the public key certificate on various tabs.

8 After you finish viewing the details, click Close > Cancel.

Viewing the CA's Self-Signed Public Key Certificate Properties

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Viewing the Organizational CA's Properties and Certificates" on page 59.
2. Start ConsoleOne.
3. Double-click the Organizational Certificate Authority object.
4. Click Certificates.
5. Click the down-arrow to see the certificates available to view.
6. Click Self-Signed Certificate.

   The property page displays the subject's fully-typed name, the issuer's fully-typed name, and the validity dates of the public key certificate.
7. To view additional information about the certificate, click Details.

   The Details page displays information contained in the public key certificate on various tabs.
8. After you finish viewing the details, click Close > Cancel.

Exporting the Organizational CA's Self-Signed Public Key Certificate

The self-signed public key certificate can be used for verifying the identity of the Organizational CA and the validity of a certificate signed by the Organizational CA.

From the Organizational CA's property page, you can view the certificates and properties associated with this object. From the self-signed certificate property page, you can export the self-signed certificate to a file for use in cryptography-enabled applications.

The self-signed certificate that resides in the Organizational CA provides the same verification of the CA's identity as a trusted root certificate that is exported from a server certificate. Any service that recognizes the Organizational CA as a trusted root will accept the self-signed or trusted root certificate as valid.

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see “Exporting the Organizational CA’s Certificate(s)” on page 59.
2. Start ConsoleOne.
3. Double-click the Organizational Certificate Authority object.
4. Click the Certificates tab.
5. Click Certificates.
6. Click the down-arrow to see the available certificates.
7. Click Self-Signed Certificate.
8. Click Export.

   This opens a wizard that helps you export the user certificate to a file.

Server Certificate Object Tasks

Creating Server Certificate Objects

This task was discussed in Chapter 2. See “Creating Server Certificate Objects” on page 20.

Importing a Public Key Certificate

You import a public key certificate after you have issued a certificate signing request (CSR) and the Certificate Authority (CA) has returned a signed public key certificate to you. This task applies when you have created a Server Certificate object using the Custom option with the External CA signing option.

The CA will return two certificates: a signed public key certificate, which verifies your identity, and a trusted root certificate, which verifies the CA's identity. These certificates can then be imported and stored in the Server Certificate object. The cryptography-enabled application that is linked to this Server Certificate object can then use this information to perform secure transactions.

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Importing a Public Key Certificate into a Server Certificate Object" on page 60.

2. Start ConsoleOne.

3. Double-click the Server Certificate object.

4. Click Import Certificates. The Import Certificates button is available from the General tab or the Certificates tab.

5. Click Import Certificates. The Import Certificates button is available from the General tab or the Certificates tab.

   - To paste the trusted root certificate into the dialog box, first use any text editor to open the certificate you received from the Certificate Authority (CA), then copy the "-----BEGIN CERTIFICATE-----" and the "-----END CERTIFICATE-----" lines and all information between them. Then, paste the certificate in the box provided in the Import Server Certificates dialog box.

   - To install the trusted root certificate from a file, click Read from File to browse for the certificate you received from the CA. Select the file, then click OK.

6. Click Next.

7. Indicate the location of the server certificate. The server certificate can be imported either by pasting it into the dialog box or by reading it from a file using the same procedure described in Step 5.

8 Click Finish.

This stores the public key certificate and the trusted root certificate in the Server Certificate object. The Certificate property page now displays the distinguished names of the subject and the issuer, as well as the validity period of the public key certificate.

9 To view the details of your newly installed public key certificate, click Details. Click Help for further information about the certificate details page.

10 Click Close > Cancel.

Your public key certificate is added to the Server Certificate object.

Exporting a Trusted Root Certificate

You export a trusted root certificate to a file so that a client (such as an Internet browser) can use it to verify the certificate chain sent by a cryptography-enabled application.

You can export a trusted root certificate in two file formats: DER encoded (.DER) and Base64 encoded (.B64). The .CRT extension can also be used for DER-encoded certificates.

If you export to the system clipboard, you can then paste the certificate directly into a cryptography-enabled application, if supported. The certificate exists on the clipboard in Base64 encoded format.

If you export to a file, you can specify either format. DER encoded format is the default format. It is the same as CRT format and can be used with applications that accept CRT formats.

1 Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see “Exporting a Trusted Root Certificate From a Server Certificate Object” on page 60.

2 Using ConsoleOne, create the Server Certificate object for the particular application.

3 Configure the application to work with the new Server Certificate object.

4. At the client where you want to run the application, start ConsoleOne, double-click the Server Certificate object, click Certificates, and click Trusted Root Certificate to go to the Trusted Root page.

5. Click Export.

6. Select the output format, the filename, and the path where you want the file to be saved.

7. Click Export.

8. Import the trusted root certificate into a cryptography-enabled application.

   For example, if you want to install a trusted root certificate in a Netscape Navigator 4.*x* browser, enter the path to the certificate in the browser's location box. This initiates a wizard that will accept the trusted root certificate and its Certificate Authority (CA) in a list of usable CAs. When this is completed, the browser will accept transactions with services that use certificates issued by this CA.

Deleting a Server Certificate Object

You should delete a Server Certificate object if you suspect that the private key has been compromised, if you no longer want to use the key pair, or if the trusted root in the Server Certificate object is no longer trusted.

IMPORTANT: Once the Server Certificate object is deleted, you will not be able to recover it. Before you delete this object, make sure that no cryptography-enabled applications still need to use it.

You can re-create a Server Certificate Object, but you will have to reconfigure any applications that referenced the old object.

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Deleting a Server Certificate Object" on page 60.

2. Start ConsoleOne.

3. Highlight the Server Certificate object that you want to delete.

4 Press Delete, then click Yes.

Viewing a Server Certificate Object's Properties

ConsoleOne allows you to view the Server Certificate object's properties. Besides the NDS rights and properties that are viewable with any NDS object, you can also view properties specific to the Server Certificate object, including the properties of the public key certificate and the trusted root certificate associated with it, if they exist.

These properties provide you with the information you need to perform any task related to this object.

1 Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Viewing the Server Certificate Object's Properties and Certificates" on page 60.

2 Start ConsoleOne.

3 Double-click the Server Certificate object.

This brings up the property pages for the Server Certificate Object, including a General page, a Certificates page, and property pages related to NDS.

4 Click the tabs that you want to view.

5 Click Cancel.

Viewing a Server Certificate Object's Public Key Certificate Properties

1 Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Viewing the Server Certificate Object's Properties and Certificates" on page 60.

2 Start ConsoleOne.

3 Double-click the Server Certificate object containing the public key certificate that you want to view.

4 Click the Certificates tab.

5 Click the down-arrow to see the certificates available to view.

6 Click Public Key Certificate.

- If a public key certificate is installed, the property page displays the subject's fully-typed name, the issuer's fully typed name, and the validity dates of the public key certificate.
- If the public key certificate has not yet been installed, the property page indicates this.

7 To view additional information about a public key certificate, click Details. The Details page displays information contained in the public key certificate on various tabs.

8 After you finish viewing the details, click Close > Cancel.

Viewing a Server Certificate Object's Trusted Root Certificate Properties

1 Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Viewing the Server Certificate Object's Properties and Certificates" on page 60.

2 Start ConsoleOne.

3 Double-click the Server Certificate object containing the trusted root certificate that you want to view.

4 Click the Certificates tab.

5 Click the down-arrow to see the certificates available to view.

6 Click the Trusted Root Certificate.

- If a trusted root certificate is installed, the property page displays the subject's fully typed name, the issuer's fully-typed name, and the validity dates of the trusted root certificate.
- If the trusted root certificate has not yet been installed, Novell Certificate Server indicates this.

7 To view additional information about an installed trusted root certificate, click Details. The Details page displays information contained in the trusted root certificate on various tabs.

8 After you finish viewing the details, click Close > Cancel.

User Certificate Tasks

Creating User Certificates

This task was discussed in Chapter 2. See "Creating User Certificates" on page 22.

Viewing a User Certificate's Properties

ConsoleOne allows you to view the user certificate's properties. Besides the NDS rights and properties that are viewable with any NDS object, you can also view properties specific to the user certificate, including the issuer, the certificate status, the private key status and the validation period.

These properties provide you with the information you need to perform any task related to this object.

1 Log in to the NDS tree as the user who owns the user certificate or as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Viewing a User Certificate's Properties" on page 60.

2 Start ConsoleOne.

3 Double-click the User object that hosts the user certificate. This brings up the property pages for the User object.

4 Click the Security tab.

5 Click on a certificate to view its properties.

6 Click Close > Cancel.

Exporting a User Certificate Using ConsoleOne

This task allows a user or network administrator to use ConsoleOne to export a user certificate for use in secure e-mail.

The user certificate can be exported with or without the private key. The network administrator or another user with sufficient rights can export a user certificate. However, only the user who owns the user certificate can export the user certificate with the private key. No other user, not even the network administrator, has rights to export a user's private key.

1 Log in to the NDS tree as the user who owns the user certificate if you are exporting the certificate and the private key. If you are only exporting the user certificate, log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Exporting a User Certificate Using ConsoleOne or Novell Certificate Console" on page 60.

2 Start ConsoleOne.

3 Double-click the User object that hosts the user certificate.

4 Click the Security tab.

5 Click on the user certificate that you want to export.

6 Click Export. This opens a wizard that helps you export the user certificate to a file.

7 Import the user certificate into a cryptography-enabled application.

Exporting a User Certificate Using Novell Certificate Console

This task allows a user to use Novell Certificate Console to export a user certificate for use in secure e-mail.

Only the user can export his or her private key. No other user, not even the network administrator, has rights to export a user's private key.

1. Set up Novell Certificate Console by running SETUP.EXE in the *install directory*\CERTCONSOLE directory and completing the installation.

   NOTE: You can also configure ZENworks™ to automate the distribution of Novell Certificate Console by using the ZENworks files that ship with Novell Certificate Server. The file CERTCNSL ZENWORKS.EXE, found in the *install directory*\CERTCONSOLE directory, is a self-extracting file that contains all the files you will need to distribute Novell Certificate Server using ZENworks.

2. Start Novell Certificate Console by double-clicking the Novell Certificate Console icon on your desktop.

3. If you are logged in as more than one user, select the appropriate user from the Current Connections pull-down menu.

   You will need to be logged in to the NDS tree as the user who owns the user certificate if you are exporting the certificate and the private key. To view the appropriate rights for this task, see "Exporting a User Certificate Using ConsoleOne or Novell Certificate Console" on page 60.

4. Click on the user certificate that you wish to export.

5. Click Export.

   This opens a wizard that helps you export the user certificate to a file.

6. Import the user certificate into a cryptography-enabled application.

Trusted Root Object Tasks

Creating a Trusted Root Container

This task was discussed in Chapter 2. See “Creating a Trusted Root Container” on page 23.

Creating Trusted Root Objects

This task was discussed in Chapter 2. See “Creating Trusted Root Objects” on page 24.

Viewing a Trusted Root Object’s Properties

ConsoleOne allows you to view the Trusted Root object’s properties. Besides the NDS rights and properties that are viewable with any NDS object, you can also view properties specific to the Trusted Root object, including the issuer, the certificate status, and the validation period.

These properties provide you with the information you need to perform any task related to this object.

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see “Viewing a Trusted Root Object’s Properties” on page 61.
2. Start ConsoleOne.
3. Open the Trusted Root Container that hosts the Trusted Root object.
4. Double-click the Trusted Root object. This brings up the property pages for the Trusted Root object.
5. Click the tabs that you wish to view.
6. Click Cancel.

Replacing a Trusted Root Certificate

This task allows you to replace a Trusted Root Certificate that is stored in the Trusted Root object. This task should be performed if the Trusted Root Certificate has expired.

You can replace a Trusted Root Certificate from the Trusted Root object's property page.

1. Log in to the NDS tree as an administrator with the appropriate rights. To view the appropriate rights for this task, see "Replacing a Trusted Root Certificate" on page 61.
2. Start ConsoleOne.
3. Open the Trusted Root Container that hosts the Trusted Root object.
4. Double-click the Trusted Root object. This brings up the property pages for the Trusted Root object.
5. Click the Trusted Root tab.
6. Click Replace. This opens the Replace a Trusted Root Certificate wizard that helps you replace the Trusted Root Certificate. For specific information on the wizard pages, click Help.
7. Click Cancel.

NDS Tasks

Merging Two Trees that Have Security Containers

In normal operation, you should never need to delete the Security container. However, if your NDS tree is to be merged with another NDS tree and both trees have a Security container, one of the Security containers must be deleted in order to successfully complete the merge.

Deleting the Security container in an NDS tree will have serious consequences for the Organizational CA and Server Certificate objects.

Do not rename the Security container, as this could lead to confusion as to which container is the real Security container for the tree. Novell Certificate Server always assumes the Security container is named *Security*.

Issues Relating to the Organizational CA

Before you can delete the Security container, you must first delete the Organizational CA object. You cannot simply move the Organizational CA to a new container.

Deleting the Organizational CA object invalidates the Organizational CA and any public key certificates it issued. These public key certificates are stored in Server Certificate objects throughout the NDS tree. Public key certificates signed by the deleted Organizational CA remain valid for a short period of time. However, these public key certificates should be replaced by new public key certificates issued by a new Organizational CA or by an external CA.

Restoring or Re-creating the Security Container

After deleting a Security container, you can restore it from backup if needed. If no backups are available, an administrator with Supervisor rights at the [Root] of the NDS tree can re-create the Security container by installing Secure Authentication Services on a server in the NDS tree. Doing so creates the Security container under [Root].

You can then create a new Organizational CA object in the Security container using ConsoleOne. You must then re-create the public key certificates signed by the previous Organizational CA and update any cryptography-enabled applications that have the previous Organizational CA's public key certificate in its list of trusted root certificates.

Resolving Multiple Security Containers, Organizational CAs, KAP Containers, and W0 Objects

Novell Certificate Server can be installed on multiple servers in an NDS tree. However, for Novell Certificate Server to function properly, only one Security container, Organizational CA, KAP container and W0 object should exist in the tree.

If you are installing Novell Certificate Server to multiple servers in an NDS tree, you must allow NDS to replicate between each installation of Novell Certificate Server. If you do not, your installation to another server may not recognize that the tree already has a Security container, an Organizational CA, a KAP container, and/or a W0 object and may recreate these objects on another server in the same NDS tree.

The items below describe possible scenarios and how to resolve them.

- If you have two or more Security containers in the same NDS Tree, and each contains an Organizational CA, a KAP container with a W0 object, do not issue any certificates. Contact Novell Technical Support for help in resolving this.

- If you have one Security container that contains two KAP containers in the same NDS tree, do not issue any certificates. Contact Novell Technical Support for help in resolving this.

- If you have one Security container that contains two Organizational CA's and one KAP container with a W0 object in the same NDS tree, delete every server and user certificate issued by both Organizational CA's. Then, delete both CA's and create a new Organizational CA.

- If you have two or more Security containers in the same NDS tree, and each contains an Organizational CA, but only one contains a KAP container with a W0 object, delete every server and user certificate issued by all Organizational CA's. Delete all the Security containers without the KAP container and W0 object. If the remaining Security container is not named *Security*, rename it to *Security*.

- If you have two or more Security containers in the same NDS tree, and only one contains an Organizational CA and a KAP container with a W0 object, delete all the Security containers without the KAP container and W0 object. If the remaining Security container is not named *Security*, rename it to *Security*.

Restoring or Re-creating a Security Container

If you delete the Security container, you will not be able to create a tree Certificate Authority until you have restored or re-created the security container.

To restore the security container, you must restore the NDS partition containing the Security container.

To recreate the Security container, use one of three methods:

- Log in as a system administrator with Create rights at the root of the NDS tree. Start ConsoleOne. Right-click on the Root container and click New > Object. From the list box in the New Object dialog box, double-click SAS:Security.

- A system administrator with Create rights at the root of the NDS tree can run SASI.NLM, if it is available. If it is not available, reinstall Novell Certificate Server 2.0 on any server in the tree.

Restoring or Re-creating KAP and W0

If you delete the KAP container and W0 object, you can restore them by restoring the NDS partition that contains these objects.

If you do not have a backup of the NDS partition, contact Novell Technical Support for help in recreating these objects.

Application Tasks

This section describes how to configure GroupWise 5.5 enhancement pack client, Outlook98, Outlook2000, and Netscape Messenger to use Novell certificates for secure e-mail. For other cryptography-enabled applications, we recommend that you consult the application's documentation for specific instructions.

The general process for enabling applications to secure e-mail is:

1. Export your Organizational CA's self-signed certificate and your user certificate to a file.
2. Import the Organizational CA's self-signed certificate into your Internet browser.
3. Import the user certificate into your e-mail client.
4. Configure your e-mail client to secure your e-mail.

Exporting the Organizational CA's Self-Signed Certificate and User Certificate

Before you can configure the cryptography-enabled applications, you will need to have the Organizational CA's self-signed certificate and a user certificate available to be imported into the applications.

See "Exporting the Organizational CA's Self-Signed Public Key Certificate" on page 30, "Exporting a User Certificate Using ConsoleOne" on page 38, and "Exporting a User Certificate Using Novell Certificate Console" on page 39.

Importing the Organizational CA's Self-Signed Certificate into Your Internet Browser

NOTE: The following Internet browsers will only recognize certificates that have been exported in .DER or a .CRT format. Though .B64 is an optional export format, it will not be recognized by these Internet browsers.

Microsoft Internet Explorer Version 4

If you are using Microsoft Internet Explorer version 4, do the following to import the Organizational CA's certificate:

1. Launch Microsoft Internet Explorer.
2. Click File > Open.
3. Enter or browse for the filename of the exported Organizational CA's self-signed certificate, then click OK.

   This opens the New Site Certificate dialog.
4. Under Available Usages, check the checkbox next to Secure E-mail, then click OK.
5. Click Yes to add the certificate to the Root Store.

Microsoft Internet Explorer Version 5

If you are using Microsoft Internet Explorer version 5, do the following to import the Organizational CA's certificate.

1. Launch Microsoft Internet Explorer.
2. Click File > Open.
3. Enter or browse for the filename of the exported Organizational CA's self-signed certificate, then click OK.

   This opens the Certificate dialog.
4. Select Install Certificate.

   This opens the Certificate Manager Import Wizard.

5. Click Next.

6. Select the area where you would like to store the certificate, then click Next > Finish > Yes.

Netscape Navigator

If you have installed either Microsoft Internet Explorer 5.*x* or NT 4 Service Pack 4 or later on your workstation, you must complete the following steps to import the Organizational CA's self-signed certificate into Netscape Navigator. This is necessary because Microsoft's products intercept opening trusted root files with a .CRT or .DER extension.

1. Double-click the file *install directory*\CERTSERV\MISC\X509.REG. This will install the .x509 extension.

2. Rename the Organizational CA's self-signed certificate file so it has an .x509 extension.

3. Launch Netscape Navigator.

4. Click File > Open Page.

5. Enter or browse for the filename of the self-signed certificate with the .x509 extension.

6. Click Open.

   The New Certificate Authority dialog should appear. If it doesn't, you have not correctly installed the .x509 extension, or you have not correctly renamed the self-signed certificate.

7. Follow the wizard. Make sure the Accept this Certificate Authority for Certifying E-mail Users check box is checked.

8. Click Next until the dialog to enter a short name for this Certificate Authority appears.

9. Click Finish.

If you have not installed either Microsoft Internet Explorer 5.*x* or NT 4 Service Pack 4 or greater, you must complete the following steps to import the Organizational CA's certificate into Netscape Navigator:

1. Launch Netscape Navigator.
2. Select File > Open Page.
3. Enter or browse for the filename of the self-signed certificate you previously exported.
4. Click Open.
5. Follow the wizard. Make sure the Accept this Certificate Authority for Certifying E-mail Users check box is checked.
6. Click Next until the dialog to enter a short name for this Certificate Authority appears.
7. Click Finish.

Importing the User Certificate into Your E-mail Client

GroupWise 5.5 Enhancement Pack Client

1. Launch GroupWise.
2. Click Tools > Options.
3. Double-click on the Certificates icon.
4. Click on Import.
5. Browse for or enter the filename of your exported user certificate.
6. Enter your password, then click OK.
7. Click on *Set Security Level* if you wish to change the default security level for your private key, then click OK.

8. To select a default certificate to use for sending signed e-mail, you can now either select the checkbox next to the certificate, or highlight the certificate and click *Set As Default*.

9. Click OK.

Microsoft Outlook 98

1. Launch Outlook™.

2. Click Tools > Options.

3. Click on the Security tab.

4. Click Import/Export Digital ID.

5. Select the Import existing Exchange or S/MIME Security Information radio button.

6. For Import File and Password, enter the filename and password of your exported user certificate.

7. For Keyset, enter a nickname. This can be any text.

8. Click OK. The private key and certificate are imported in to Outlook98.

Microsoft Outlook2000

This procedure applies to Outlook2000 with Microsoft Internet Explorer version 5.

1. Launch Outlook.

2. Click Tools > Options.

3. Click on the Security tab.

4. Click Import/Export Digital ID.

5. Select the Import existing Exchange or S/MIME Security Information radio button.

6. For Import File and Password, enter the filename and password of your exported user certificate.

7. For Digital ID Name, enter a nickname. This can be any text.

8. If you are prompted to add the Organizational CA certificate to the Root Store, click Yes.

Netscape Messenger 4.*x*

1. Launch Netscape Messenger.

2. Click the New Msg icon.

3. Double-click the Security icon on the Navigation toolbar.

4. Click Certificates > Yours.

5. Click Import a Certificate. If a password was entered to protect the Communicator Certificate database, enter it.

6. Enter or browse for the filename of the user certificate you exported previously.

7. Enter the password you selected to protect the user certificate's private key.

8. Click OK.

Configuring Your E-mail Client to Secure Your E-mail

GroupWise 5.5 Enhancement Pack Client

You will need to have imported at least one certificate and key into GroupWise in order to make use of signed e-mail. You will need to have a certificate available for each recipient to which you would like to send encrypted e-mail.

1. Launch GroupWise.

2. Click Tools > Options.

3. Double-click the Security icon.

4. Click the Send Options tab.

5. To enable signing as default for all outgoing e-mail, click the check box next to *Sign digitally using*. You can then select a different certificate to use by clicking on the Certificate drop-down list underneath this option.

6. To enable encryption as default for all outgoing e-mail, click on the check box next to *Encrypt for recipients using*. You can then select the encryption method by clicking on the Method drop-down list underneath this option. The available encryption methods depend on the security service provider you have selected.

7. To select a different Security Service Provider, click on the Name drop down list underneath this option. You can then select from one of the installed security service providers displayed in this list. Then, click OK.

From an item view (send mail, post message, task, reminder note, etc.), you can change the default security options for this particular item by selecting File > Properties and clicking on the Security tab. From here you can change the signing and encryption options.

From an item view (send mail, post message, task, reminder note, etc.), you can also toggle the selection of either signing or encryption for this particular item by clicking on the Encrypt or Digitally Sign icons at the top of the view.

Microsoft Outlook

1. Launch Outlook.

2. Click Tools > Options.

3. Click the Security tab.

4. Click Setup Secure E-mail or Change Settings, depending on whether you have previously entered security settings.

5. Select S/MIME for the Secure Message Format.

6. Click the Choose button on the Signing Certificate line.

7. Select the certificate that you will use for digitally signing e-mail that you send to others, then click OK.

8. Click the Choose button on the Encryption Certificate line.

9. Select the certificate that others will use for encrypting e-mail that they send to you, then click OK.

10. Check the Send These Certificates with Signed Message check box, then click OK.

11. Select whatever combination of options you prefer in the Secure E-mail section, then click OK.

Netscape Messenger

1. Launch Netscape Messenger.

2. Click the New Msg icon.

3. Click the Security icon.

4. Click Messenger.

5. Select the certificate you will use for digitally signing your e-mail that you send to others under the Certificate Signed and Encrypted Messages heading.

   You can select other options as desired on this page. Refer to the Netscape help topics for further information on these options and their purposes.

A Public Key Cryptography Basics

Overview

The content of most Internet communications, such as Web page browsing or public chat forums, can be monitored by anyone equipped to do so. The content of other data transmissions, such as the exchange of credit card information for online purchases, needs to be kept private.

Public key cryptography is a widely used method for keeping data transmissions private and secure on the Internet. Specifically, public key cryptography is the system of using digital codes called "keys" to authenticate senders of messages and to encrypt message content.

Secure Transmissions

Data transmissions are private and secure when two things happen:

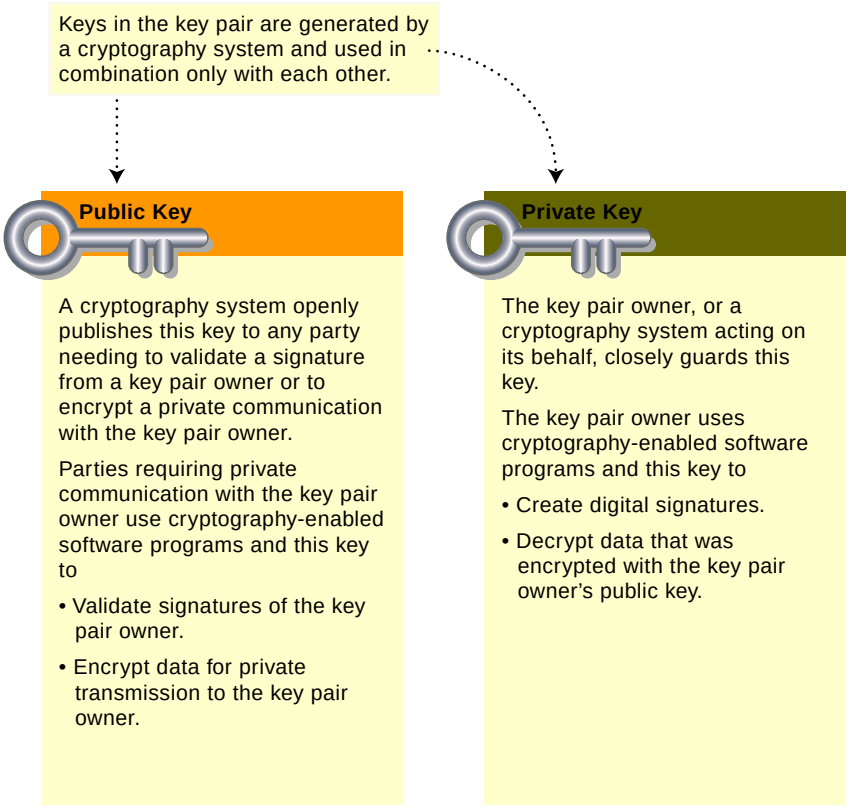
- **Authentication** —The data receiver knows that the data sender is exactly who or what it claims to be.
- **Encryption** —The data sent is encrypted so that it can be read only by the intended receiver.

Key Pairs

Authentication and encryption are both provided through the use of mathematically related pairs of digital codes or “keys.” One key in each pair is publicly distributed; the other is kept strictly private.

Each data transmitter, whether a person, a software program, or some other entity such as a bank or business, is issued a key pair by a public key cryptography system.

The basic principles and functions of each key in the key pair are summarized in the following illustration.



Key Pairs and Authentication

Authentication means that the data receiver knows that the data sender is exactly who or what it claims to be.

Suppose that you want to authorize your bank to transfer funds from your account to another account. The bank needs proof that the message came from you and that it has not been altered during transit. The following illustrates the process that your online transaction would follow using public key cryptography.

1. You authorize the transfer using your banking application.
2. Your application creates a "digital signature" for the transfer request using your *private* key (which only your application can access).
3. The application then sends the request and your digital signature to your bank.

4. Your bank's computer receives the request and your digital signature.
5. A system operator then validates your signature against the request using your *public* key.

If the results compute correctly, the signature is "authenticated."

If not, the signature, the message, or both are assumed to be fraudulent, and the transaction is denied.

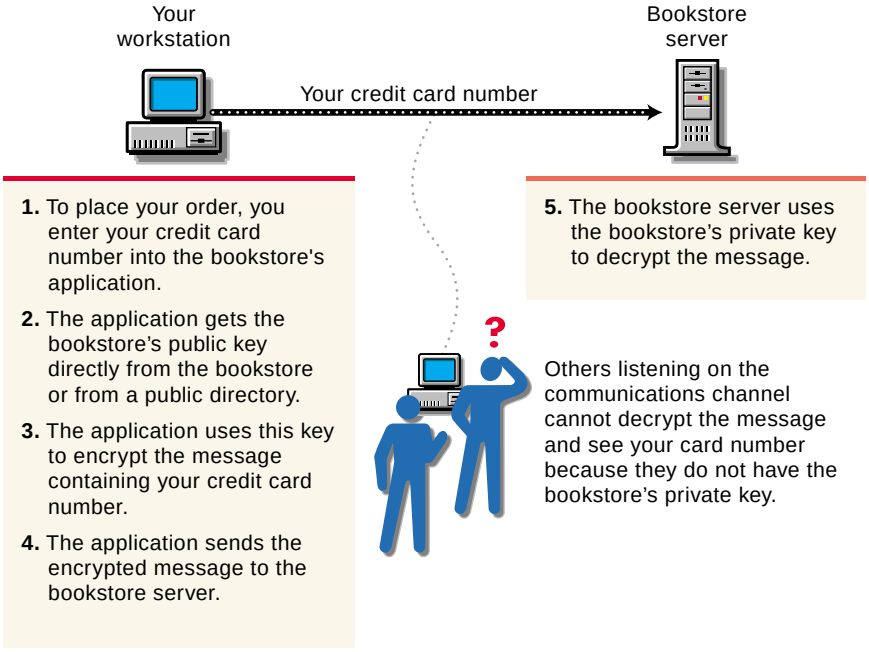
For information about digital signatures and their verification, see "Digital Signatures" on page 57 .

Key Pairs and Encryption

Encryption means that the data can be read only by the intended receiver.

Suppose you want to order a book from an Internet vendor and you need to use your credit card to pay for it. You don't want your credit card number read by anyone other than the intended recipient.

The encryption process in the following illustration provides the mechanisms through which your credit card number can be safely transmitted.



Establishing Trust

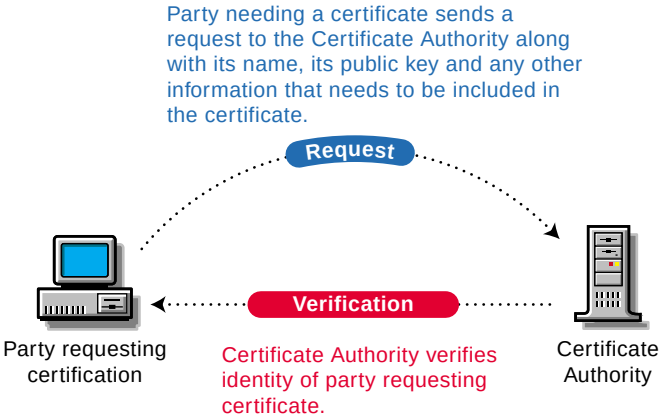
If a sender and receiver know and trust each other, they can simply exchange public keys and establish secure data transmission, including authentication and encryption. To do this, they would use each other's public keys and their own private keys.

Under normal circumstances, however, parties needing secure data transmissions have no foundation for trusting the identity of each other. Each needs a third party, whom they both trust, to provide proof of their identity.

Certificate Authorities

A party needing to prove its identity in a public key cryptography environment enlists the services of a trusted third party known as a certificate authority.

The primary purpose of the certificate authority is to verify that a party is who or what it claims to be, and then to issue a public key certificate for that party to use. The public key certificate verifies that the public key contained in the certificate belongs to the party named in the certificate.

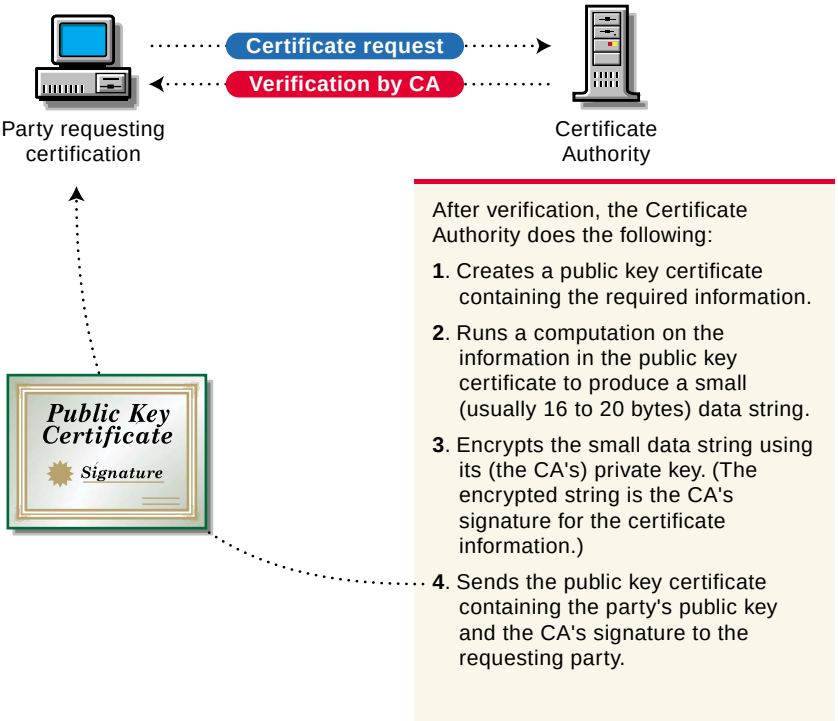


Once the identity of the requesting party has been established to the satisfaction of the certificate authority, the certificate authority‘ issues an electronic “certificate” and applies its digital signature.

Digital Signatures

Just as a personal signature applied to a paper document indicates the authenticity of the document, a digital signature indicates the authenticity of electronic data.

To create a digital signature, the software used to create the signature links the data being signed with the private key of the signer. The following illustration shows the process that a CA follows to create its digital signature for a public key certificate.



A digital signature is uniquely linked to the signer and the data. No one else can duplicate the signature because no one else has the signer's private key. In addition, the signer cannot deny having signed the data. This is known as *non-repudiation*.

When a certificate authority signs a public key certificate, it guarantees that it has verified the identify of the public key owner according to the certificate authority's established and published policies.

After signed data (such as a public key certificate) is received, software verifies data authenticity by applying the same computation to the data that the signing software used originally. If the data is unaltered, both computations will produce identical results. It can then be safely assumed that neither the data nor the signature was modified in transit.

B

Entry Rights Needed to Perform Tasks

This listing provides the specific entry rights an administrator needs to manage Novell Certificate Server® tasks within an NDS® tree. These rights are the minimum entry rights needed.

This listing should also be helpful to the administrator who would like to grant rights to another user to manage part or all of company's certificate authority and certificate management needs.

Tasks	Entry Rights Needed
Install Novell Certificate Server	For the first install to an NDS Tree: • Supervisor at the Root of the Tree For subsequent installs: • Browse to the W0 object
Creating an Organizational CA	• Supervisor on the Security container
Viewing the Organizational CA's Properties and Certificates	• Browse on the Organizational CA's object
Exporting the Organizational CA's Certificate(s)	• Browse on the Organizational CA's object
Issuing a Public Key Certificate	• Read to the *NDSPKI:Private Key* on the Organizational CA's object

Tasks	Entry Rights Needed
Creating Server Certificate Objects	• Supervisor on the server's container • Read to the attribute *NDSPKI:Private Key* on the Organizational CA's object
Importing a Public Key Certificate into a Server Certificate Object	• Write to the attribute *NDSPKI:Public Key Certificate* on the Server Certificate Object • Write to the attribute *NDSPKI:Certificate Chain* on the Server Certificate Object
Deleting a Server Certificate Object	• Delete on the container that holds the Server Certificate Object
Exporting a Trusted Root Certificate From a Server Certificate Object	• Browse on the Server Certificate Object
Viewing the Server Certificate Object's Properties and Certificates	• Browse on the Server Certificate Object
Creating User Certificates	• Read to the attribute *NDSPKI:Private Key* on the Organizational CA object • Read and Write to the attribute *NDSPKI:userCertificateInfo* on the user object • Read and Write to the attribute *SAS:SecretStore* on the user object • Read and Write to the attribute *userCertificate* on the user object
Viewing a User Certificate's Properties	• Browse on the user object
Exporting a User Certificate Using ConsoleOne or Novell Certificate Console	• Browse on the user object

Tasks	Entry Rights Needed
Exporting a User's Private Key and Certificate Using ConsoleOne and Novell Certificate Console	• You must be logged in as the user.
Creating a Trusted Root Container	• Create on the Security container
Creating Trusted Root Objects	• Create on the Trusted Root Container in which the Trusted Root object will reside
Viewing a Trusted Root Object's Properties	• Browse on the Trusted Root Object
Replacing a Trusted Root Certificate	• Read and Write to *NDSPKI:Not After* on the Trusted Root object • Read and Write to *NDSPKI:Not Before* on the Trusted Root object • Read and Write to *NDSPKI:Subject Name* on the Trusted Root object • Read and Write to *NDSPKI:Trusted Root Certificate* on the Trusted Root object
Creating a Security Container	• Create on the Root of the NDS tree