End-Entity Online Help

Sun™ ONE Certificate Server

Version 4.7

September 2002
816-5545-10
Second Edition

Copyright © 2002 Sun Microsystems, Inc. All rights reserved.

Sun, Sun Microsystems, and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Federal Acquisitions: Commercial Software -- Government Users Subject to Standard License Terms and Conditions.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation. No part of the product or this document may be reproduced in any form by any means without prior written authorization of the Sun Microsystems, Inc. and its licensers, if any.

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Some pre-existing portions:

Copyright © 1998,1999 by Jef Poskanzer <jef@acme.com>. All rights reserved. Copyright © 1996 by Jef Poskanzer <jef@acme.com>. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) "HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT "LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright © 2002 Sun Microsystems, Inc. Tous droits réservés.

Sun, Sun Microsystems, le Sun logo, et iPlanet sont des marques dposes ou des marques dposes registre de Sun Microsystems, Inc. aux Etats-Unis et d'autres pays.

Le produit dé crit dans ce document est distribué selon des conditions de licence qui en restreignent l'utilisation, la copie, la distribution et la décompilation.

Aucune partie de ce produit ni de ce document ne peut être reproduite sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite préalable de Sun Microsystems, Inc., le cas échéant, de ses bailleurs de licence.

CETTE DOCUMENTATION EST FOURNIE "EN L'ÉTAT", ET TOUTES CONDITIONS EXPRESSES OU IMPLICITES, TOUTES REPRÉSENTATIONS ET TOUTES GARANTIES, Y COMPRIS TOUTE GARANTIE IMPLICITE D'APTITUDE À LA VENTE, OU À UN BUT PARTICULIER OU DE NON CONTREFAÇON SONT EXCLUES, EXCEPTÉ DANS LA MESURE OÙ DE TELLES EXCLUSIONS SERAIENT CONTRAIRES À LA LOI.

Contents

Chapter 1

Understanding Certificates

This guide describes how to get a new certificate, renew an existing certificate, and perform other operations with iPlanet Certificate Management Server (CMS). It is intended for users and server administrators who are not familiar with certificates or with Certificate Management System.

NOTE Sun™ ONE Certificate Server was previously known as iPlanet™ Certificate Management System. The product was renamed shortly before the launch of this 4.7 release.

The late renaming of this product has resulted in a situation where the new product name is not fully integrated into the shipping product. In particular, you will see the product referenced as iPlanet Certificate Management Server within the product GUI and within the product documentation. For this release, please consider iPlanet Certificate Management Server and Sun™ ONE Certificate Server as interchangeable names for the same product.

The following sections introduce you to basic concepts that will help you understand certificates and use Certificate Management System. For brief definitions of terms, see the *Glossary*.

- Internet Security Issues
- Encryption and Decryption
- Public-Key Cryptography
- Digital Signatures
- Certificates
- What You Do with Certificate Management System

Internet Security Issues

Communication over the Internet uses the Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP allows information to be sent from one computer to another through a variety of intermediate computers and separate networks before it reaches its destination.

The great flexibility of TCP/IP has led to its worldwide acceptance as the basic Internet and intranet communications protocol. At the same time, the fact that TCP/IP allows information to pass through intermediate computers makes it possible for a third party to interfere with communications in the following ways:

- **Eavesdropping.** Information remains intact, but its privacy is compromised. For example, someone could learn your credit card number, record a sensitive conversation, or intercept classified information.
- **Tampering.** Information in transit is changed or replaced and then sent on to the recipient. For example, someone could alter an order for goods or change a person's resume.
- **Impersonation.** Information passes to a person who poses as the intended recipient. Impersonation can take two forms:
    - **Spoofing.** A person can pretend to be someone else. For example, a person can pretend to have the email address `jdoe@mozilla.com`, or a computer can identify itself as a site called `www.mozilla.com` when it is not. This type of impersonation is known as spoofing.
    - **Misrepresentation.** A person or organization can misrepresent itself. For example, suppose the site `www.mozilla.com` pretends to be a furniture store when it is really just a site that takes credit-card payments but never sends any goods.

Normally, users of the many cooperating computers that make up the Internet or other networks don’t monitor or interfere with the network traffic that continuously passes through their machines. However, many sensitive personal and business communications over the Internet require precautions that address the threats listed above. Fortunately, some well-established techniques and standards collectively known as *public-key cryptography* make it relatively easy to take such precautions.

Public-key cryptography and related techniques facilitate the following tasks:

- **Encryption and decryption** allow two communicating parties to disguise information they send to each other. The sender encrypts, or scrambles, information before sending it. The receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder.
- **Tamper detection** allows the recipient of information to verify that it has not been modified in transit. Any attempt to modify data or substitute a false message for a legitimate one will be detected.
- **Authentication** allows the recipient of information to determine its origin--that is, to confirm the sender's identity.
- **Nonrepudiation** prevents the sender of information from claiming at a later date that the information was never sent.

The sections that follow introduce the concepts of public-key cryptography that underlie these capabilities.

Encryption and Decryption

Encryption is the process of scrambling information so it is unintelligible to anyone but the intended recipient. *Decryption* is the process of unscrambling encrypted information so that it is intelligible again. A *cryptographic algorithm,* also called a *cipher,* is set of rules or directions used to encrypt or decrypt data. In most cases, two related algorithms are employed, one for encryption and the other for decryption.

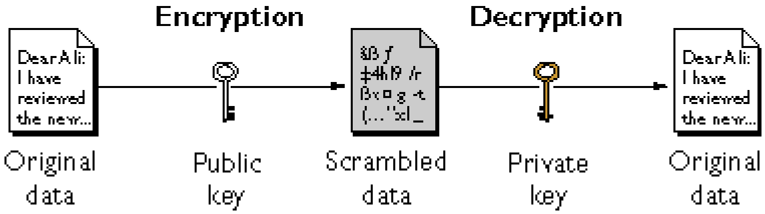
With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, which is widely known, but on a number called a *key* that must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple. Decryption without the correct key is very difficult, and in some cases impossible for all practical purposes.

Public-Key Cryptography

Public-key cryptography is the name for some well-established techniques and standards that allow an entity to verify its identity electronically or to sign and encrypt electronic data. It involves a pair of keys--a *public key* and a *private key*--associated with the entity. The most commonly used implementations of public-key cryptography are based on algorithms patented by RSA Data Security. Therefore, this section describes the RSA approach.

Each public key is published, and the corresponding private key is kept secret. Data encrypted with your public key can be decrypted only with your private key. Figure 1-1 shows a simplified view of the way public-key encryption works.

Figure 1-1 Public-key encryption



The scheme shown in Figure 1-1 lets you freely distribute a public key, and only you will be able to read data encrypted using this key. In general, to send encrypted data to someone, you encrypt the data with that person’s public key, and the person receiving the encrypted data decrypts it with the corresponding private key.

As it happens, the reverse of the scheme shown in Figure 1-1 also works: data encrypted with your private key can be decrypted only with your public key. This would not be a desirable way to encrypt sensitive data, however, because it means that anyone with your public key, which is by definition published, could decrypt the data. Nevertheless, private-key encryption is useful, because it means you can use your private key to sign data with your digital signature--an important requirement for electronic commerce and other commercial applications of cryptography. Client software such as Communicator can then use your public key to confirm that the message was signed with your private key and that it hasn’t been tampered with since being signed.

Digital Signatures

Encryption and decryption address the problem of eavesdropping, one of the three Internet security issues mentioned at the beginning of this chapter. But encryption and decryption, by themselves, do not address the other two problems mentioned in Internet Security Issues: tampering and impersonation.

This section describes how public-key cryptography addresses the problem of tampering. The section that follows describes how it addresses the problem of impersonation.

Tamper detection and related authentication techniques rely on a mathematical function called a *one-way hash* (also called a *message digest*). A one-way hash is a number of fixed length with the following characteristics:

- The value of the hash is unique for the hashed data. Any change in the data, even deleting or altering a single character, results in a different value.
- The content of the hashed data cannot, for all practical purposes, be deduced from the hash--which is why it is called “one-way.”

As mentioned in Public-Key Cryptography, it’s possible to use your private key for encryption and your public key for decryption. Although this is not desirable when you are encrypting sensitive information, it is a crucial part of digitally signing any data. Instead of encrypting the data itself, the signing software creates a one-way hash of the data, then uses your private key to encrypt the hash. The encrypted hash, along with other information, such as the name of the hashing algorithm, is known as a *digital signature.*

Figure 1-2 shows a simplified view of the way a digital signature can be used to validate the integrity of signed data.

Figure 1-2 Using a digital signature to validate data integrity

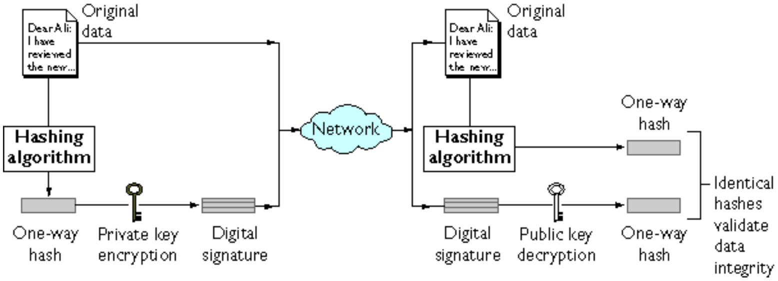


Figure 1-2 shows two items transferred to the recipient of some signed data: the original data and the digital signature, which is basically a one-way hash (of the original data) that has been encrypted with the signer's private key. To validate the integrity of the data, the receiving software first uses the signer's public key to decrypt the hash. It then uses the same hashing algorithm that generated the original hash to generate a new one-way hash of the same data. (Information about the hashing algorithm used is sent with the digital signature, although this isn't shown in the figure.) Finally, the receiving software compares the new hash against the original hash. If the two hashes match, the data has not changed since it was signed. If they don't match, the data may have been tampered with since it was signed, or the signature may have been created with a private key that doesn't correspond to the public key presented by the signer.

If the two hashes match, the recipient can be certain that the public key used to decrypt the digital signature corresponds to the private key used to create the digital signature. Confirming the identity of the signer, however, also requires some way of confirming that the public key really belongs to a particular person or other entity. Digital identification documents called certificates, which are described in the next section, address this issue.

The significance of a digital signature is comparable to the significance of a handwritten signature. Once you have signed some data, it is difficult to deny doing so later--assuming that the private key has not been compromised or out of the owner's control. This quality of digital signatures provides a high degree of nonrepudiation--that is, digital signatures make it difficult for the signer to deny having signed the data. In some situations, a digital signature may be as legally binding as a handwritten signature.

Certificates

A *certificate* is an electronic document used to identify an individual, a server, a company, or some other entity and to associate that identity with a public key. Like a driver's license, a credit card, a passport, or other commonly used personal IDs, a certificate provides generally recognized proof of a person's identity. Public-key cryptography uses certificates to address the problem of impersonation (see Internet Security Issues).

To get a driver's license, you typically apply to a government agency, such as the Department of Motor Vehicles, which verifies your identity, your ability to drive, your address, and other information before issuing the license. To get a credit card, you apply to a company that performs a credit check before issuing the ID. To get a library card, you may need to provide only your name and a utility bill with your address on it.

Certificates work much the same way as any of these familiar forms of identification. *Certificate authorities (CAs)* are entities that validate identities and issue certificates. They can be either independent third parties or organizations running their own certificate-issuing server software (such as Certificate Management System). The methods used to validate an identity vary depending on the policies of a given CA—just as the methods to validate other forms of identification vary depending on who is issuing the ID and the purpose for which it will be used. In general, before issuing a certificate, the CA must use published verification procedures to ensure that an entity requesting a certificate is in fact who it claims to be.

The certificate issued by the CA binds a particular public key to the name of the entity the certificate identifies (such as the name of an employee). Certificates help prevent the use of fake public keys for impersonation. Only the public key certified by the certificate will work with the corresponding private key possessed by the entity identified by the certificate.

In addition to a public key, a certificate always includes the name of the entity it identifies, an expiration date, the name of the CA that issued the certificate, a serial number, and other information. Most importantly, a certificate always includes the digital signature of the issuing CA. The CA's digital signature allows the certificate to function as a "letter of introduction" for users who know and trust the CA but don't know the entity identified by the certificate.

What You Do with Certificate Management System

Certificate Management System allows you to perform the following tasks:

- **Enrollment.** You can apply for and obtain a certificate for yourself or for a server that you administer. See “User Enrollment.”and “Server Enrollment.”
- **Renewal.** You can renew a certificate that is about to expire or has already expired. See “User Certificate Renewal.”
- **Revocation.** If you are a system administrator, you can revoke a certificate so that it is no longer valid. See “User Certificate Revocation.”
- **Retrieval.** You can list all certificates that are available to you or to your server. See “Certificate Retrieval.”

Chapter 2

Using Certificate Management System

With iPlanet Certificate Management Server (CMS), you can perform the following tasks:

- User Enrollment
- Server Enrollment
- Registration Manager Enrollment
- Certificate Manager Enrollment
- OCSP Responder Enrollment
- WTLS Certificate Enrollment
- Object Signing Enrollment
- CMC Request Enrollment
- User Certificate Renewal
- User Certificate Revocation
- Certificate Retrieval
- Import CA Certificate Chain
- Import Certificate Revocation List

For an introduction to basic terms and concepts, see , “Understanding Certificates.”

User Enrollment

Certificate Management System provides forms that support several kinds of user enrollment:

- Manual User Enrollment (based on explicit approval by someone who verifies the user’s identity)
- Directory-Based User Enrollment (based on user information in an LDAP directory)
- Directory- and PIN-Based Enrollment (based on user information and an identifying PIN number in a directory)
- NIS Enrollment (based on user information in a NIS name service)
- Portal Enrollment (based on a user providing information and selecting a user name that is unique in the portal directory)
- Certificate-Based Enrollment (based on a user providing a pre-issued certificate)

Additional enrollment forms may be available at your site.

Manual User Enrollment

When you enroll manually, you submit all the information Certificate Management System needs to create a certificate for you. This information is then evaluated by a person who may use a variety of means to confirm your identity (physical proof, information gathered over the telephone, and so on). This person then decides whether to issue the certificate. Because you must wait for someone to review and approve your request, it can take some time before your certificate is issued.

Fill out the enrollment form as directed. If you are not sure how to supply some of the information, ask your system administrator. When you are sure everything is correct, click the Submit button at the bottom of the form.

When the enrollment request is approved, you will receive an email notification that includes the certificate and instructions for importing it into your browser.

For an introduction to basic terms and concepts, see , “Understanding Certificates.”

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

Organization Unit, Organization, and Country. These attributes are combined with your name and login ID to form a unique identifier called your distinguished name. Ask your system administrator for specific designations for your organization unit and organization. Depending on how your system is configured, you may not need to provide all of these attributes.

Challenge Phrase Password. The challenge phrase is a password that you can use to revoke or renew your certificate at any time. In order to revoke or renew the certificate, you must either present the certificate to the server (your web browser will do this automatically if the certificate is installed in it) or you must know this secret challenge phrase (in case your certificate is not accessible when you need to revoke or renew it, or the certificate that you want to renew is a server or object signing certificate). Select a password that you can remember and use a mix of letters, numbers, and symbols (for example, !,@,#,%,^). Protect your password: if someone else knows it, they can revoke or renew your certificate.

Contact Information. This information is used to verify your identity and to direct the certificate to you when it is issued.

Additional Comments. You may be able to provide comments that will help the issuing agent confirm your identity and decide whether to approve your request.

Key-length Information. The key length determines the encryption strength of your key. The United States and other governments have set rules governing permissible encryption strengths in data or software that is imported or exported, so the key length you use may be dictated by which countries you are dealing with. If you are not sure what key length to use, ask your system administrator.

Directory-Based User Enrollment

If your organization has a Lightweight Directory Access Protocol (LDAP) directory, the directory contains much of the information that Certificate Management System needs to verify your identity and issue a certificate. The directory-based user enrollment form uses such a directory.

Fill out the enrollment form as directed. If you are not sure how to supply some of the information, ask your system administrator. When you are sure everything is correct, click the Submit button at the bottom of the form.

Upon receiving the request and confirming the information you provided with an LDAP directory, Certificate Management System issues the certificate automatically and immediately. If the certificate is successfully issued, your new certificate will appear in a browser window, along with instructions on how to import it into your browser.

For an introduction to basic terms and concepts, see , “Understanding Certificates.”

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

IMPORTANT NOTICE TO ADMINISTRATORS. If you see text at the top of the form that says IMPORTANT NOTICE TO ADMINISTRATORS, you should immediately contact your system administrator. If this text is present, the form probably won’t work, and your administrator may not have set up Certificate Management System and the LDAP directory correctly.

User’s Identity. Enter the user name and password you use to log on to the network or to the directory.

Key-length Information. The key length determines the encryption strength of your key. The United States and other governments have set rules governing permissible encryption strengths in data or software that is imported or exported, so the key length you use may be dictated by which countries you are dealing with. If you are not sure what key length to use, ask your system administrator.

Directory- and PIN-Based Enrollment

If your organization has a Lightweight Directory Access Protocol (LDAP) directory, the directory contains much of the information that Certificate Management System needs to verify your identity and issue a certificate. Before you enroll, your system administrator sends you a unique personal identification number (PIN) that helps guarantee your identity. This is the number you must enter in the enrollment form.

Fill out the enrollment form as directed, using the PIN you have received. If you are not sure how to supply some of the information, ask your system administrator. When you are sure everything is correct, click the Submit button at the bottom of the form.

Upon receiving the request and confirming the information you provided, Certificate Management System issues the certificate automatically and immediately. If the certificate is successfully issued, your new certificate will appear in a browser window, along with instructions on how to import it into your browser.

For an introduction to basic terms and concepts, see , “Understanding Certificates.”

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

IMPORTANT NOTICE TO ADMINISTRATORS. If you see text at the top of the form that says IMPORTANT NOTICE TO ADMINISTRATORS, you should immediately contact your system administrator. If this text is present, the form probably won't work, and your administrator may not have set up Certificate Management System and the LDAP directory correctly.

User's Identity. Enter the user name and password you use to log on to the network or to the directory. Also enter the PIN provided to you for enrolling for a certificate.

Key-length Information. The key length determines the encryption strength of your key. The United States and other governments have set rules governing permissible encryption strengths in data or software that is imported or exported, so the key length you use may be dictated by which countries you are dealing with. If you are not sure what key length to use, ask your system administrator.

NIS Enrollment

NIS or NIS+ is a network information name service. If your organization uses NIS to store information about users, the NIS service contains much of the information that Certificate Management System needs to verify your identity and issue a certificate.

You need to provide the user name and password you use to log into the network. When you are sure everything is correct, click the Submit button at the bottom of the form.

Upon receiving the request and confirming the information you provided, Certificate Management System issues the certificate automatically and immediately. If the certificate is successfully issued, your new certificate will appear in a browser window, along with instructions on how to import it into your browser.

For an introduction to basic terms and concepts, see , "Understanding Certificates."

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

User's Identity. Enter the user name and password you use to log on to the NIS-based network or server.

Key-length Information. The key length determines the encryption strength of your key. The United States and other governments have set rules governing permissible encryption strengths in data or software that is imported or exported, so the key length you use may be dictated by which countries you are dealing with. If you are not sure what key length to use, ask your system administrator.

Portal Enrollment

Portal enrollment allows you to enroll for a certificate when you register yourself with a portal. My Sun is an example of a portal. See http://mysun.sun.com. You only need to provide a user name that is unique on the portal, a new password, and whatever personal information the portal operator needs to issue a certificate to you (for example, your name and address).

Fill out the enrollment form as directed. When you are sure everything is correct, click the Submit button at the bottom of the form.

You may be asked to re-submit the form if any of the required information is missing or if the user name is already in use.

Upon receiving a valid request and confirming the information you provided, Certificate Management System issues the certificate automatically and immediately. If the certificate is successfully issued, your new certificate will appear in a browser window, along with instructions on how to import it into your browser.

For an introduction to basic terms and concepts, see , "Understanding Certificates."

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

User's Identity. Select a user name (or enter the user name you have already registered) and enter a new password. To keep the password secret, it does not appear as you type it (you see only asterisks) so you need to enter it twice: the entries are compared to make sure you typed the same thing in both fields.

User's Personal Information. This section asks for more information that is needed to issue a certificate to you. Be sure to fill out all fields that are required. In the default form, these fields are marked with an asterisk.

Key-length Information. The key length determines the encryption strength of your key. The United States and other governments have set rules governing permissible encryption strengths in data or software that is imported or exported, so the key length you use may be dictated by which countries you are dealing with.

Certificate-Based Enrollment

In this method of enrollment, you submit a pre-issued certificate as an authentication token to obtain a new certificate. The certificate is pre-issued to you by your company, and you cannot enroll for the new certificate without the pre-issued certificate. If you don't have the pre-issued certificate, contact your administrator.

For certificate-based enrollment, the following forms are provided:

- Certificate Based User Enrollment for Dual Certs - Directory Based
- Certificate Based User Enrollment for Encryption Certs - Directory Based
- Certificate Based User Enrollment for Single Certs - Directory Based

You might be using one of these forms and it might be customized to suit your organization's policies and procedures. Hence, the form you see may not include all the elements explained for a form.

Fill out the enrollment form as directed. If you are not sure how to supply some of the information, ask your system administrator. When you are sure everything is correct, click the Submit button at the bottom of the form.

Upon receiving the request and confirming the information you provided with your company's directory, Certificate Management System issues the certificate automatically and immediately. If the certificate is successfully issued, your new certificate will appear in a browser window, along with instructions on how to import it into your browser.

For an introduction to basic terms and concepts, see , "Understanding Certificates."

Certificate Based User Enrollment for Dual Certs - Directory Based

This form enables you to request dual certificates—one for signing and another for encryption—by submitting the pre-issued certificates as authentication tokens.

User's Identity. In this section, enter your user ID and password for your organization's directory. This information will be used to verify your identity and to obtain information from the directory to fill in the certificate details.

Certificate Based User Enrollment for Encryption Certs - Directory Based

This form enables you to request an encryption certificate by submitting the pre-issued certificate as an authentication token.

User's Identity. In this section, enter your user ID and password for your organization's directory. This information will be used to verify your identity and to obtain information from the directory to fill in the certificate details.

Public/Private Key Information. The key length determines the encryption strength of your key. The United States and other governments have set rules governing permissible encryption strengths in data or software that is imported or exported, so the key length you use may be dictated by which countries you are dealing with. If you are not sure what key length to use, ask your system administrator.

Certificate Based User Enrollment for Single Certs - Directory Based

This form enables you to request a signing certificate by submitting the pre-issued certificate as an authentication token.

User's Identity. In this section, enter your user ID and password for your organization's directory. This information will be used to verify your identity and to obtain information from the directory to fill in the certificate details.

Public/Private Key Information. The key length determines the encryption strength of your key. The United States and other governments have set rules governing permissible encryption strengths in data or software that is imported or exported, so the key length you use may be dictated by which countries you are dealing with. If you are not sure what key length to use, ask your system administrator.

Server Enrollment

Certificate Management System provides a manual enrollment form for server enrollment; manual enrollment is based on explicit approval by someone who verifies the server's identity. Additional enrollment forms may be available at your site.

Server Certificate Enrollment (for Server Administrators)

This form is intended for use by server administrators. Before a server can support the Secure Sockets Layer (SSL) protocol for authentication, encryption, and tamper detection, it must have an SSL server certificate.

When you enroll manually for an SSL server certificate, you submit all the information Certificate Management System needs to create the certificate. This information is then evaluated by a person who may use a variety of means to confirm your identity (physical proof, information gathered over the telephone, and so on). This person then decides whether to issue the certificate. Because you must wait for someone to review and approve your request, it can take some time before your certificate is issued.

Fill out the enrollment form as directed. If you are not sure how to supply some of the information, ask your system administrator. When you are sure everything is correct, click the Submit button at the bottom of the form.

When the enrollment request is approved, you will receive an email notification that includes either the certificate itself or a URL at which you can find the certificate. You must copy the encoded certificate and import it into your server. (For an iPlanet server, use the administration forms provided by the Administration Server associated with your server.)

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

PKCS #10 Request. If you are the administrator for an iPlanet server, create the PKCS #10 request using the Administration Server associated with the server for which you are requesting a certificate. In the Administration Server's administration forms, choose Encryption, then choose Request Server Certificate. If you are not using an iPlanet server, use your server's tools for creating a PKCS#10 request.

Challenge Phrase Password. The challenge phrase is a password that you can use to revoke or renew your certificate at any time. In order to revoke or renew the certificate, you must either present the certificate to the server (your web browser will do this automatically if the certificate is installed in it) or you must know this secret challenge phrase (in case your certificate is not accessible when you need to revoke or renew it, or the certificate that you want to renew is a server or object signing certificate). Select a password that you can remember and use a mix of letters, numbers, and symbols (for example, !,@,#,%,^). Protect your password: if someone else knows it, they can revoke or renew your certificate.

Server Administrator Contact Information. This information is used to verify your identity and to direct the certificate to you when it is issued.

Additional Comments. You may be able to provide comments that will help the issuing agent confirm your identity and decide whether to approve your request.

Registration Manager Enrollment

This form is intended for use by agents who are managing a Registration Manager. Registration Managers must have a signing certificate issued by the Certificate Manager for which the Registration Manager is handling end-entity interactions. This form allows Registration manager agents to enroll for such a certificate. This type of enrollment is always manual; that is, the request must be approved by the human agent responsible for the Certificate Manager.

Fill out the enrollment form as directed. When the enrollment request is approved, you will receive an email notification that includes the certificate or a URL at which you can find the certificate. You must copy the certificate and import it into the Registration Manager from the CMS window in iPlanet Console.

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

PKCS #10 Request. The PKCS #10 certificate request that you need to paste here is created during installation of the Registration Manager.

Challenge Phrase Password. The challenge phrase is a password that you can use to revoke or renew your certificate at any time. In order to revoke or renew the certificate, you must either present the certificate to the server (your web browser will do this automatically if the certificate is installed in it) or you must know this secret challenge phrase (in case your certificate is not accessible when you need to revoke or renew it, or the certificate that you want to renew is a server or object signing certificate). Select a password that you can remember and use a mix of letters, numbers, and symbols (for example, !,@,#,%,^). Protect your password: if someone else knows it, they can revoke or renew your certificate.

Server Administrator Contact Information. This information is used to identify you in case the administrator needs to contact you and to direct the certificate to you when it is issued.

Additional Comments. You may be able to provide comments that will help the issuing agent confirm your identity and decide whether to approve your request.

Certificate Manager Enrollment

This form is intended for use by agents who are managing a Certificate Manager that is to be used as a subordinate CA. A Certificate Manager that functions as a subordinate CA must have a signing certificate issued by the Certificate Manager to which it is subordinate. This type of enrollment is always manual; that is, the request must be approved by the human agent responsible for the Certificate Manager that will be issuing the certificate.

Fill out the enrollment request form as directed. When the enrollment request is approved, you will receive an email notification that includes the certificate or a URL at which you can find the certificate. You must copy the certificate and import it into the subordinate Certificate Manager, using iPlanet Console's CMS window.

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

PKCS #10 Request. The PKCS #10 certificate request that you need to paste here is created during installation of the Certificate Manager for which you are requesting a signing certificate.

Challenge Phrase Password. The challenge phrase is a password that you can use to revoke or renew your certificate at any time. In order to revoke or renew the certificate, you must either present the certificate to the server (your web browser will do this automatically if the certificate is installed in it) or you must know this secret challenge phrase (in case your certificate is not accessible when you need to revoke or renew it, or the certificate that you want to renew is a server or object signing certificate). Select a password that you can remember and use a mix of letters, numbers, and symbols (for example, !,@,#,%,^). Protect your password: if someone else knows it, they can revoke or renew your certificate.

Server Administrator Information. This information is used to find your entry in the directory and to identify you in case an administrator needs to contact you.

Additional Comments. You may be able to provide comments that will help the issuing agent confirm your identity and decide whether to approve your request.

OCSP Responder Enrollment

This form is intended for use by administrators of Online Certificate Status Protocol (OCSP) Responder servers, for example, the Online Certificate Status Manager or any third-party OCSP responder. An OCSP responder requires a certificate for signing its responses to requests about certificate validity. Use this form to enroll for the OCSP Responder's signing certificate.

To enroll for a certificate for a third-party OCSP responder, follow the vendor's instructions for generating a certificate signing request and then paste that request in this enrollment form.

When you enroll manually for an OCSP Responder signing certificate, you submit all the information Certificate Management System needs to create the certificate. This information is then evaluated by a person who may use a variety of means to confirm your identity (physical proof, information gathered over the telephone, and so on). This person then decides whether to issue the certificate. Because you must wait for someone to review and approve your request, it can take some time before your certificate is issued.

When the enrollment request is approved, you will receive an email notification that includes either the certificate itself or a URL at which you can find the certificate. You must copy the encoded certificate and import it into your server.

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

PKCS #10 Request. Use your server's tools for creating a PKCS#10 request, copy the request to the clipboard, and then paste the request in this section of the form.

Challenge Phrase Password. The challenge phrase is a password that you can use to revoke or renew your certificate at any time. In order to revoke or renew the certificate, you must either present the certificate to the server (your web browser will do this automatically if the certificate is installed in it) or you must know this secret challenge phrase (in case your certificate is not accessible when you need to revoke or renew it, or the certificate that you want to renew is a server or object signing certificate). Select a password that you can remember and use a mix of letters, numbers, and symbols (for example, !,@,#,%,^). Protect your password: if someone else knows it, they can revoke or renew your certificate.

Server Administrator Contact Information. This information is used to verify your identity and to direct the certificate to you when it is issued.

Additional Comments. You may be able to provide comments that will help the issuing agent confirm your identity and decide whether to approve your request.

WTLS Certificate Enrollment

Certificate Management System provides two types of enrollment forms for requesting certificates for wireless devices or applications:

- WTLS User Enrollment
- Server WTLS Certificate Enrollment (for Server Administrators)

WTLS User Enrollment

This form is intended for use to request wireless certificates via the browser. This type of enrollment is always *manual*.

When you enroll manually, you submit all the information Certificate Management System needs to create a certificate for you. This information is then evaluated by a person who may use a variety of means to confirm your identity (physical proof, information gathered over the telephone, and so on). This person then decides whether to issue the certificate. Because you must wait for someone to review and approve your request, it can take some time before your certificate is issued.

Fill out the enrollment form as directed. If you are not sure how to supply some of the information, ask your system administrator. When you are sure everything is correct, click the Submit button at the bottom of the form.

When the enrollment request is approved, you will receive an email notification that includes the certificate and instructions for importing it into your browser.

For an introduction to basic terms and concepts, see , “Understanding Certificates.”

The default form elements are listed below; the form you see is customized for your site and may not include all the elements explained here.

User's Identity. Use this section to identify yourself. Enter values for the fields you want to have in your certificate. Your site may require you to fill in certain fields (* = required field). Attributes such as organization unit, organization, and so on are combined with your name and login ID to form a unique identifier called your *distinguished name*. If you are in doubt, ask your system administrator for specific designations for your organization unit and organization. Depending on how your system is configured, you may not need to provide all of these attributes.

`Full name`—Type your full name, for example, `Jane Doe`.

`Login name`—Type your login name, for example, `jdoe`.

`Email address`—Type your email address, for example, `jdoe@siroe.com`.

`Organization unit`—Type the name of the organization unit to which you belong, for example, `Sales`.

`Organization`—Type the name of your organizational or company, for example, `Siroe Corporation`.

`Country`—Type the two-letter code for your country, for example, `US`.

Challenge Phrase Password. The challenge phrase is a password that you can use to revoke your certificate at any time. In order to revoke the certificate, you must either present the certificate to the server (your web browser will do this automatically if the certificate is installed in it) or you must know this secret challenge phrase (in case your certificate is not accessible when you need to revoke it).

`Password`—Type a password that you can remember and use a mix of letters, numbers, and symbols (for example, `!,@,#,%,^`). Protect your password: if someone else knows it, they can revoke your certificate.

`Confirm password` —Type the same password again.

Additional Comments. Use this section to type any comments that you may have. For example, you may be able to provide comments that will help the issuing agent confirm your identity and decide whether to approve your request.

Public/Private Key Information. Use this section to specify the key length for your certificate. The key length determines the encryption strength of your key. The United States and other governments have set rules governing permissible encryption strengths in data or software that is imported or exported, so the key length you use may be dictated by which countries you are dealing with. If you are not sure what key length to use, ask your system administrator.

`Key length`—Select the key length. The default choices are: 1024 (High Grade), 768 (Medium Grade), and 512 (Low Grade).

Server WTLS Certificate Enrollment (for Server Administrators)

This form is intended for use by administrators to request certificates for wireless applications by submitting certificate requests in PKCS#10 format. This type of enrollment is always manual; that is, the request must be approved by the agent (a person) responsible for the Certificate Manager that will be issuing the certificate.

Fill out the enrollment request form as directed. When the enrollment request is approved, you will receive an email notification that includes the certificate or a URL at which you can find the certificate. You must copy the certificate and import it into the server that generated the certificate request.

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

PKCS #10 Request. The PKCS #10 certificate request that you need to paste here is created by the application for which you are requesting a certificate.

Server Administrator Information. This information is used to contact you, in case an administrator needs to contact you.

Additional Comments. You may be able to provide comments that will help the issuing agent confirm your identity and decide whether to approve your request.

Object Signing Enrollment

Certificate Management System provides two types of enrollment forms for requesting object signing certificates:

- Object Signing (Browser)
- Object Signing (PKCS10)

Object Signing (Browser)

This form is intended for use by administrators or software developers who want to enroll for an object-signing certificate. The keys will be generated and stored by the web browser. If you want to enroll for a certificate to use with a signing tool that does not use the browser's database (for example, the Java `keytool`), you can use the Object Signing (PKCS10) form to submit a generic PKCS #10 request for an object-signing certificate.

Object-signing certificates are used to create digital signatures that can be attached to software objects such as Java applets. Digital signatures provide recipients of such objects with some assurance that you are really the person or company responsible for the object, rather than an imposter.

This type of enrollment is always manual. After you submit all the information Certificate Management System needs to create an object-signing certificate for you, the information is evaluated by a person who may use a variety of means to identify you (physical proof, information gathered over the telephone, and so on). This person then decides whether to issue the certificate. Because you must wait for someone to review and approve your request, it can take some time before your certificate is issued.

Fill out the enrollment request form as directed. If you are not sure how to supply some of the information, ask your system administrator.

When the enrollment request is approved, you will receive an email notification that includes the certificate and instructions for importing it into your browser.

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

Organization Unit, Organization, and Country. These attributes are combined with your name and login ID to form a unique identifier called your distinguished name. Ask your system administrator for specific designations for your organization unit and organization. Depending on how your system is configured, you may not need to provide all of these attributes.

Select Signing Type. Netscape Object-Signing and Microsoft Authenticode signing require different certificate extensions in the signer's certificate. Select the option that corresponds to the object-signing protocol you use.

Challenge Phrase Password. The challenge phrase is a password that you can use to revoke or renew your certificate at any time. In order to revoke or renew the certificate, you must either present the certificate to the server (your web browser will do this automatically if the certificate is installed in it) or you must know this secret challenge phrase (in case your certificate is not accessible when you need to revoke or renew it, or the certificate that you want to renew is a server or object signing certificate). Select a password that you can remember and use a mix of letters, numbers, and symbols (for example, !,@,#,%,^). Protect your password: if someone else knows it, they can revoke or renew your certificate.

Contact Information. This information is used to verify your identity and to direct the certificate to you when it is issued.

Key-length Information. The key length determines the encryption strength of your key. The United States and other governments have set rules governing permissible encryption strengths in data or software that is imported or exported, so the key length you use may be dictated by which countries you are dealing with. If you are not sure what key length to use, ask your system administrator.

Additional Comments. You may be able to provide comments that will help the issuing agent confirm your identity and decide whether to approve your request.

Object Signing (PKCS10)

This form is intended for use by administrators or software developers who want to enroll for an object-signing certificate. This form accepts a generic PKCS #10 request. When the certificate has been issued, you can retrieve it (see Certificate Retrieval) in base-64 encoded format and import it into your object-signing application (for example, the Java `keytool`). To enroll for a Netscape Object-Signing certificate (for use with the `signtool` application that comes with CMS) or a Microsoft Authenticode signing certificate, you should use the Object Signing (Browser) form.

Object-signing certificates are used to create digital signatures that can be attached to software objects such as Java applets. Digital signatures provide recipients of such objects with some assurance that you are really the person or company responsible for the object, rather than an imposter.

This type of enrollment is always manual. After you submit all the information Certificate Management System needs to create an object-signing certificate for you, the information is evaluated by a person who may use a variety of means to identify you (physical proof, information gathered over the telephone, and so on). This person then decides whether to issue the certificate. Because you must wait for someone to review and approve your request, it can take some time before your certificate is issued.

Fill out the enrollment request form as directed. If you are not sure how to supply some of the information, ask your system administrator.

When the enrollment request is approved, you will receive an email notification that includes the certificate and instructions for importing it into your browser.

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

PKCS #10 Request. Use the tools that come with your object-signing application to create a PKCS#10 request, copy the request to the clipboard, and then paste the request in this section of the form.

Select Signing Type. Netscape Object-Signing and Microsoft Authenticode signing require different certificate extensions in the signer's certificate. Select the option that corresponds to the object-signing protocol you use.

Challenge Phrase Password. The challenge phrase is a password that you can use to revoke or renew your certificate at any time. In order to revoke or renew the certificate, you must either present the certificate to the server (your web browser will do this automatically if the certificate is installed in it) or you must know this secret challenge phrase (in case your certificate is not accessible when you need to revoke or renew it, or the certificate that you want to renew is a server or object signing certificate). Select a password that you can remember and use a mix of letters, numbers, and symbols (for example, !,@,#,%,^). Protect your password: if someone else knows it, they can revoke or renew your certificate.

Contact Information. This information is used to verify your identity and to direct the certificate to you when it is issued.

Additional Comments. You may be able to provide comments that will help the issuing agent confirm your identity and decide whether to approve your request.

CMC Request Enrollment

This form is intended for use by administrators to submit a certificate request in the Certificate Management Messages over CMS (CMC) format for any of the following certificates:

- User / Client certificate
- SSL server certificate
- Certificate Manager's CA signing certificate
- Registration Manager's signing certificate
- OCSP responder's signing certificate

For example, during the installation of a Certificate Manager (without the ability of issuing wTLS certificates), Registration Manager, Data Recovery Manager, and Online Certificate Status Manager, one can generate the certificate request in the CMC format, instead of the widely used PKCS #10 format. Note that on two occasions, one doesn't get to choose the request format, CMC or PKCS #10, for the certificate being generated: if the Certificate Manager is enabled for issuing wTLS certificates (certificates for wireless applications / devices), the wizard doesn't give the option of generating a CMC request for the CA signing certificate; similarly, one doesn't get to choose the request format for the Online Certificate Status Manager signing certificate. In both the cases, the request will be in the PKCS #10 format.

If you choose to generate the request in the CMC format, to submit the request to a CA you may either use the Installation Wizard's auto-submission feature—a feature that enables you to send the request directly to a remote Certificate Manager or Registration Manager without having to manually copy the base-64 encoded and paste the request in an enrollment form—or manually copy the CMC request and paste it into the text area provided in this enrollment form.

When you enroll manually for a certificate based on the CMC request format, you submit all the information Certificate Management System needs to create the certificate. This information is then evaluated by a person who may use a variety of means to confirm your identity (physical proof, information gathered over the telephone, and so on). This person then decides whether to issue the certificate. Because you must wait for someone to review and approve your request, it can take some time before your certificate is issued.

When the enrollment request is approved, you will receive an email notification that includes either the certificate itself or a URL at which you can find the certificate. You must copy the encoded certificate and import it into your browser or server.

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

CMC Full Enrollment Request. Use your server's tools for creating a CMC request, copy the request to the clipboard or a text file, and then paste the request in this section of the form.

Select Certificate Type. Select a certificate type that corresponds to the certificate request you pasted in the text area:

- `User Certificate`—select this if the request you pasted is for a client certificate.
- `SSL Server Certificate`—select this if the request you pasted is for a SSL server certificate.
- `CA Signing Certificate`—select this if the request you pasted is for a subordinate Certificate Manager's CA signing certificate.
- `RA Signing Certificate`—select this if the request you pasted is for a Registration Manager's signing certificate.
- `OCSP Responder Signing Certificate`—select this if the request you pasted is for an OCSP responder's signing certificate.

Challenge Phrase Password. The challenge phrase is a password that you can use to revoke or renew your certificate at any time. In order to revoke or renew the certificate, you must either present the certificate to the server (your web browser will do this automatically if the certificate is installed in it) or you must know this secret challenge phrase (in case your certificate is not accessible when you need to revoke or renew it, or the certificate that you want to renew is a server or object signing certificate). Select a password that you can remember and use a mix of letters, numbers, and symbols (for example, !,@,#,%,^). Protect your password: if someone else knows it, they can revoke or renew your certificate.

Contact Information. This information is used to verify your identity and to direct the certificate to you when it is issued.

Additional Comments. You may be able to provide comments that will help the issuing agent confirm your identity and decide whether to approve your request.

User Certificate Renewal

The Certificate Renewal page requires SSL client authentication, so it is only available on SSL-enabled CMS servers. If you do not see the Renewal tab, ask your system administrator for the SSL-enabled URL for CMS at your site.

Certificates have a starting date and an expiration date, just like your driver's license and credit cards. When the expiration date of your certificate approaches, you must renew the certificate.

You may receive an email notification that a certificate is about to expire and must be renewed. The message may include a link to this page, which you use to request the renewal.

User Certificate

If the certificate to be renewed is a user certificate and you still have access to the certificate, you can use this form to present it to the server (using SSL client authentication) to have it renewed.

Be sure you are renewing the certificate from the same computer and browser that you used when you acquired the certificate. This is the computer on which your private key is stored.

You cannot use this form unless you have reached it via the URL for the HTTPS port of Certificate Management System. The URL in the Location field near the top of the window in which the form appears should begin with https://. If it doesn't, the form won't work, and you should ask your system administrator for the correct URL.

Certificate Renewal Using a Challenge Password

You can use this form to renew any certificate if you know the challenge phrase that was set during certificate enrollment. The challenge phrase allows you to renew your certificate even though you may no longer have access to the actual certificate (for example, if your certificate was stored on a disk that failed) or the certificate is a server or object-signing certificate which you cannot use it for SSL client authentication. You must know the challenge phrase and the certificate serial number. See "Search Certificates" for information on how to search for your certificate's serial number.

About the Form Elements

Certificate Serial Number. See Search Certificates for information on how to search for your certificate's serial number.

Authentication Information. The Challenge Password was set when you enrolled for the certificate. If you do not know the challenge password, you will not be able to use this form to renew your certificate. Contact the Certificate Management System administrator t o get your certificate renew.

For an introduction to basic terms and concepts, see , "Understanding Certificates."

User Certificate Revocation

The Certificate Revocation pages are only available on SSL-enabled CMS servers. If you do not see the Revocation tab, ask your system administrator for the SSL-enabled URL for CMS at your site.

User Certificate

You may need to revoke a certificate if, for example, it is superseded by another one or if you no longer use the service for which it is required.

If you still have access to the certificate, you can use this form to present it to the server (using SSL client authentication) to have it revoked.

For an introduction to basic terms and concepts, see , “Understanding Certificates.”

About the Form Elements

The form you see is customized for your site and may not include all the elements explained below.

Revocation Reason. Select the reason for the revocation. The reason is stored with the revoked certificate, where it can be reviewed by an administrator.

Certificate Revocation Using a Challenge Password

You may need to revoke a certificate if it is superseded by another one or if you no longer use the service for which it is required.

You can use this form to revoke any certificate if you know the challenge phrase that was set during certificate enrollment. The challenge phrase allows you to revoke your certificate even though you may no longer have access to the actual certificate (for example if you r certificate was stored on a disk that failed). You must know the challenge phrase and the certificate serial number. See “Search Certificates” for information on how to search for your certificate’s serial number.

For an introduction to basic terms and concepts, see “Understanding Certificates.”

About the Form Elements

The form you see is customized for your site and may not include all the elements explained below.

Certificate Serial Number. See “Search Certificates” for information on how to search for your certificate’s serial number.

Authentication Information. The Challenge Password was set when you enrolled for the certificate. If you do not know the challenge password, you will not be able to use this form to revoke your certificate. Contact the Certificate Management System administrator to get your certificate revoked.

Revocation Reason. Select the reason for the revocation. The reason is stored with the revoked certificate, where it can be reviewed by an administrator.

Certificate Retrieval

You may need to find one or more certificates. For example, if you want to send encrypted email, you must have the recipients’ certificates. The retrieval feature lets you search for any certificate that is in the Certificate Management System database.

The Retrieval tab allows you to perform the following tasks:

- Check Request Status: Check on the status of a pending enrollment request.
- List Certificates: Retrieve certificates by serial number
- Search Certificates: Find certificates by their owner or validity information.

- Import CA Certificate Chain: Retrieve the Certificate Manager's own identifying certificate.
- Import Certificate Revocation List: Review or update your local copy of the certificate revocation list (CRL).

For an introduction to basic terms and concepts, see , "Understanding Certificates."

Check Request Status

This form allows you to check the status of a certificate request. When you submit a request that requires manual processing, you get a request identifier from the Certificate Authority or Registration Authority where you made the request.

Enter the request identifier for a pending enrollment in the field on this form and click Submit.

If the certificate request is still pending or has been rejected, you will get a status message.

If the certificate has been issued, you will get a page showing the certificate information. At the bottom of the page there is an Import Certificate button to click to import the certificate into your browser.

List Certificates

This form allows you to list certificates by serial number.

For an introduction to basic terms and concepts, see , "Understanding Certificates."

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

Serial Number Range. You can enter a serial number in hexadecimal form, as it appears in the certificate display (a number preceded by `0x`), or in decimal form.

- ❍ If you know the specific serial number of the certificate you want, enter it in both the "Lowest Serial Number" and "Highest Serial Number" fields.
- ❍ To find all certificates within a range of serial numbers, enter the lowest and highest numbers of the range. If you leave either the lower limit or upper limit field blank, all certificates before or after the one you specify are displayed.

If you are searching within a range of serial numbers, you can choose to filter out certificates that are not currently valid. To do so, click one or both of the checkboxes at the bottom of the form.

Search Certificates

Use the form as directed. It is quite long; scroll down to see the different sections. When you have specified the search criteria, scroll to the bottom of the form and click Find.

For an introduction to basic terms and concepts, see , "Understanding Certificates."

About the Form Elements

The form you see is customized for your site and may not include all the elements explained here.

Serial Number Range. You can enter a serial number in hexadecimal form, as it appears in the certificate display (a number preceded by `0x`), or in decimal form.

- If you know the specific serial number of the certificate you want, enter it in both the "Lowest Serial Number" and "Highest Serial Number" fields.
- To find all certificates within a range of serial numbers, enter the lowest and highest numbers of the range. If you leave either the lower limit or upper limit field blank, all certificates before or after the one you specify are displayed.

Subject Name. Enter values for one or more of these fields to find certificates by their owner information. When you have entered the field values for the server to match, go to the bottom of this section to specify the type of search (Exact or Partial) that you want performed.

Email address—Narrow the search by email address.

Common name—Find certificates associated with a specific person or server.

UserID—The UserID for the person whose certificate you want to find. For example, at many companies the UserID is the name used to log in to the network when starting up a computer.

Organization unit—Narrow the search to a specific division, department, or unit within an organization.

Organization—Narrow the search to a specific business, university, or organization.

Locality—Narrow the search to a local area (for example, the name of a city).

State—Narrow the search to a state or province.

Country—Narrow the search by country. Enter a two-letter code (for example, US).

If you select the Partial match method, you can specify wildcard patterns by using the question mark character (?) to match an arbitrary single character and the asterisk character (*) to match an arbitrary string of zero or more characters. A single asterisk in a field specifies that the corresponding component must be in the certificate's subject name but may have any value. A blank field indicates that you do not care if the component is present.

Revocation Information. Find certificates that have been revoked during a particular period or by a particular agent. For example, you can search for all certificates revoked between July 1996 and January 1997, or all certificates revoked by the agent with the user name `admin`.

- To find certificates revoked within a particular time period, select the day, month, and year from the drop-down lists to identify the beginning and ending dates.
- To find certificates revoked by a particular agent, enter the name of the agent. You can use wildcards in this field.

Issuing Information. Find certificates that have been issued during a particular period or by a particular agent. For example, you can search for all certificates issued between July 1996 and January 1997, or all certificates issued by the agent with the user name `betatest`.

- To find certificates issued within a time period, select the day, month, and year from the drop-down lists to identify the beginning and ending dates.
- To find certificates issued by a particular agent, enter the name of the agent. You can use wildcards in this field.

Dates of Validity. Find certificates that become effective or expire during a particular period. For example, you can list all certificates that became valid on June 1, 1996, or that will expire between January 1, 2001 and June 1, 2001.

You can also list certificates that have a validity period of a certain length of time. For example, you can list all certificates that are valid for less than one month.

- To find certificates that become effective or expire within a time period, select the day, month, and year from the drop-down lists to identify the beginning and ending dates.

- To find certificates that have a validity period of a certain length of time, select "Not greater" or "Not less" from the drop-down list, enter a number, and select a time unit from the drop-down list: Days, Weeks, Months, or Years.

Type. Find certain types of certificates—that is, those that are intended for a particular use. For example, you can search for all certificates for subordinate CAs.

For each usage type, choose whether to find certificates where that type is On, Off, or Absent. If you leave the usage type blank, that type is not considered in the search.

Note that the type search works only for certificates containing the `netscape-cert-type` extension, which stores type information.

Import CA Certificate Chain

Before you can use any certificate that you receive, the certificate authority (CA) that signed it must be in your browser's list of trusted CAs. That CA's certificate may in turn be signed by another CA. There can be a whole chain of subordinate CAs, all the way to a root CA. At least one of the CAs in the chain must be trusted in order for you to use the certificate. To add a CA to your list of trusted CAs, you import the CA's certificate or certificate chain into your browser.

When you begin to use Certificate Management System as your local CA, you must import its certificate chain into your browser in order to use certificates that it issues. Similarly, if you are a server administrator, you must import the certificate chain into the server in order for that server to accept client authorization certificates signed by that Certificate Management System.

Use this form to import the certificate chain for Certificate Management System into your browser or into a server you manage. You need to do this only once, when you first begin using Certificate Management System.

For an introduction to basic terms and concepts, see , “Understanding Certificates.”

About the Form Elements

The form you see is customized for your site and may not include all the elements explained below.

Users. Options listed this section are for downloading the CA certificate chain into a browser.

- Import the CA certificate chain into your browser—This imports the certificate chain for Certificate Management System into your browser's list of trusted CAs. This option works for most browsers.
- Download the CA certificate chain in binary form—If your browser does not use the standard importation format or procedure, use this option to save the chain as a binary file and import it by some other method.
- Download the wTLS CA certificate in binary form—Use this option to save the Wireless Transport Layer Security (wTLS) CA certificate as a binary file and import it into the wireless application by some other method.

Administrators. Options listed this section are for downloading the CA certificate chain into a server.

- Display the CA certificate chain in PKCS#7 for importing into a server—This displays the entire certificate chain on your screen in PKCS #7 format, so that you can copy and paste it to import it into a server you manage. For iPlanet servers, use the Administration Server associated with the server to import the chain.
- Display certificates in the CA certificate chain for importing individually into a server—For a server that does not accept the PKCS #7 format for certificate chains, this displays each certificate in the chain separately, so that you can import each one into the server.

Import Certificate Revocation List

Your browser may automatically import the latest certificate revocation list (CRL) from an LDAP directory that receives regular updates from Certificate Management System, and it may automatically check all certificates against the CRL to ensure that they have not been revoked. If your browser does not do this automatically, or if you have reason to believe that the CRL is out of date (if your computer or the LDAP directory has been down, for example), use this form to check the master CRL or update the browser's version.

For an introduction to basic terms and concepts, see , "Understanding Certificates."

About the Form Elements

The form you see is customized for your site and may not include all the elements explained below.

Check whether the following certificate is revoked. Use this option to manually check the revocation status of a particular certificate if you are not sure whether you have the latest version of the CRL. Enter the serial number of the certificate in decimal form, or in hexadecimal form (preceded by `0x`) as it appears in the certificate display.

Import the latest CRL to your Netscape Navigator. If you are using Netscape Navigator or Netscape Communicator, use this option to automatically download and import the latest version of the CRL into your browser.

Download the latest CRL in binary form. If you are not using Netscape Navigator or Netscape Communicator, use this option to save a binary form of the latest CRL to a local file. You can import this file into your browser by whatever method is appropriate.

Display the CRL header information. The header of the master CRL published by Certificate Management System contains the date and time of the latest update. You can compare this information to that in your browser's CRL to see if you have the latest version.

Glossary

authentication Confident identification; that is, assurance that a party to some computerized transaction is not an impostor. Authentication typically involves the use of a password, certificate, personal identification number (PIN), or other information that can be used to validate identity over a computer network. See also password-based authentication, certificate-based authentication, client authentication, server authentication.

CA See certificate authority (CA).

CA certificate A certificate that identifies a certificate authority. See also certificate authority (CA), subordinate CA, root CA.

certificate Digital data that specifies the name of an individual, company, or other entity and certifies that a public key, which is also included in the certificate, belongs to that entity. A certificate is issued and digitally signed by a certificate authority (CA). A certificate's validity can be verified by checking the CA's digital signature. See also public-key cryptography.

certificate authority (CA) A trusted entity that issues a certificate after verifying the identity of the person or entity the certificate is intended to identify. A CA also renews and revokes certificates and generates a list of revoked certificates at regular intervals. CAs can be independent third parties (such as the CAs listed at Certificate Authority Services) or a person or organization using certificate-issuing server software (such as iPlanet Certificate Management System). See also certificate revocation list (CRL).

certificate-based authentication Verification of identity based on certificates and public-key cryptography. See also password-based authentication.

certificate chain A hierarchical series of certificates signed by successive certificate authorities. A CA certificate identifies a certificate authority (CA) and is used to sign certificates issued by that authority. A CA certificate can in turn be signed by the CA certificate of a parent CA and so on up to a root CA.

certificate fingerprint A unique, fixed-length number associated with a certificate. The number is not part of the certificate itself but is produced by applying a mathematical function to the contents of the certificate. If the contents of the certificate change, even by a single character, the function produces a different number. Certificate fingerprints can therefore be used to verify that certificates have not been tampered with.

Certificate Management Messages over CMS (CMC) A general interface to public-key certification products based on Cryptographic Message Syntax (CMS) and PKCS #10, including a certificate enrollment protocol for DSA-signed certificates with Diffie-Hellman public keys. A proposed standard from the IETF PKIX working group. CMC incorporates CRMF and CMMF. Future versions of Certificate Management System will support this standard as it is finalized.

certificate revocation list (CRL) A list of revoked certificates that is generated and signed by a certificate authority (CA). You can download the latest CRL to your browser or to a server, then check against it to make sure that certificates are still valid before permitting their use for authentication.

cipher See cryptographic algorithm.

client authentication The process of identifying a client to a server, for example with a name and password or with a client SSL certificate and some digitally signed data. See also Secure Sockets Layer (SSL), server authentication.

client SSL certificate A certificate that a client (for example, browser software such as Netscape Communicator) presents to a server to authenticate its identity using the Secure Sockets Layer (SSL) protocol. See also client authentication.

Cryptographic Message Syntax (CMS) A superset of PKCS #7 syntax used for digital signatures and encryption. A proposed standard from the IETF PKIX working group.

cryptographic algorithm A set of rules or directions used to perform cryptographic operations such as encryption and decryption.

decryption The process of unscrambling data that has been encrypted. See also encryption.

digital ID See certificate.

digital signature A code created from both the data to be signed and the private key of the signer. This code is unique for each new piece of data. Even a single comma added to a message changes the digital signature for that message. Successful validation of your digital signature by appropriate software not only provides evidence that you approved the transaction or message, but also provides evidence that the data has not changed since you digitally signed it. See also nonrepudiation, tamper detection.

distinguished name (DN) A specially formatted name that uniquely identifies the subject of a certificate.

dual key pair Two public-private key pairs--four keys altogether--corresponding to two separate certificates. The private key of one pair is used for signing operations, and the public and private keys of the other pair are used for encryption and decryption operations. Each pair corresponds to a separate certificate. See also public-key cryptography.

eavesdropping Surreptitious interception of information sent over a network by an entity for which the information is not intended.

encryption The process of scrambling information in a way that disguises its meaning. For example, encrypted connections between computers make it very difficult for third-parties to unscramble, or *decrypt*, information flowing over the connection. Encrypted information can be decrypted only by someone who possesses the appropriate key. See also public-key cryptography.

encryption key A private key used for encryption only. An encryption key and its equivalent public key, plus a signing key and its equivalent public key, constitute a dual key pair.

fingerprint See certificate fingerprint.

impersonation Posing as the intended recipient of information sent over a network. Impersonation can take two forms: spoofing and misrepresentation.

key A large number used by a cryptographic algorithm to encrypt or decrypt data. A person's public key, for example, allows other people to encrypt messages to that person. The encrypted messages must be decrypted with the corresponding private key. See also public-key cryptography.

Lightweight Directory Access Protocol (LDAP) A protocol for accessing directory services.

misrepresentation Presentation of an entity as a person or organization that it is not. For example, a web site might pretend to be a furniture store when it is really just a site that takes credit card payments but never sends any goods. Misrepresentation is one form of impersonation. See also spoofing.

iPlanet Certificate Management System A highly configurable set of software components and tools for creating, deploying, and managing certificates. You enroll with the system to obtain certificates of all kinds; the system maintains information about the certificates it issues.

nonrepudiation The inability by the sender of a message to deny having sent the message at a later time. A regular hand-wrtten signature provides on form of nonrepudiation. A digital signature provides another.

object signing A technology that allows software developers to sign Java code, JavaScript scripts, or any kind of file, and allows users to identify the signers and control access by signed code to local system resources.

object-signing certificate A certificate whose corresponding private key is used to sign objects such as code files. See also object signing.

password-based authentication Confident identification by means of a name and password. See also authentication.

private key One of a pair of keys used in public-key cryptography. The private key is kept secret and is used to decrypt data that has been encrypted with the corresponding public key.

public key One of a pair of keys used in public-key cryptography. The public key is distributed freely and published as part of a certificate. It is typically used to encrypt data sent to the public key's owner, who then decrypts the data with the corresponding private key.

public-key cryptography Well-established techniques and standards that allow an entity to verify its identity electronically or to sign and encrypt electronic data. Two keys are involved: a public key and a private key. The public key is published as part of a certificate, which associates that key with a particular identity. The corresponding private key is kept secret. Data encrypted with the public key can be decrypted only with the private key.

public-key infrastructure (PKI) The standards and services that facilitate the use of public-key cryptography and certificates in a networked environment.

root CA The certificate authority (CA) with a self-signed certificate at the top of a certificate chain. See also subordinate CA.

Secure Sockets Layer (SSL) A protocol that allows mutual authentication between a client and server for the purpose of establishing an authenticated and encrypted connection. SSL runs above TCP/IP and below HTTP, LDAP, IMAP, NNTP, and other high-level network protocols. See also authentication, encryption.

server authentication The process of identifying a server to a client by using a server SSL certificate. See also client authentication, Secure Sockets Layer (SSL).

server SSL certificate A certificate that a server presents to a client to authenticate the server's identity using the Secure Sockets Layer (SSL) protocol.

signing certificate A certificate whose corresponding private key is used to sign transmitted data, so that the receiver can verify the identity of the sender. See also digital signature.

signing key A private key used for signing only. A signing key and its equivalent public key, together with an encryption key and its equivalent public key, constitute a dual key pair.

spoofing Pretending to be someone else. For example, a person can pretend to have the email address `jdoe@mozilla.com`, or a computer can identify itself as a site called `www.mozilla.com` when it is not. Spoofing is one form of impersonation. See also misrepresentation.

SSL See Secure Sockets Layer (SSL).

subject The entity identified by a certificate. In particular, the subject field of a certificate contains a unique representation of the certified entity's name and other characteristics.

subject name A distinguished name (DN) that uniquely describes the subject of a certificate.

subordinate CA A certificate authority (CA) whose certificate is signed by another subordinate CA or by the root CA. See also certificate chain, root CA.

symmetric encryption An encryption method that uses the same cryptographic key to encrypt and decrypt a given message.

tamper detection A mechanism ensuring that data received in electronic form has not been tampered with; that is, that the data received entirely corresponds with the original version of the same data.

trust Confident reliance on a person or other entity. In the context of public-key infrastructure (PKI), trust refers to the relationship between the user of a certificate and the certificate authority (CA) that issued the certificate. If you trust a CA, you can generally trust valid certificates issued by that CA. You typically control which CAs you trust and which you don't, and thet kinds of certificates you trust them to issue, by means of settings within your browser or server software.