



"What is a Certificate?" and Related Topics

[Security Home Page](#)

ALERTS

[Current Network Blocks](#)
[Critical Vulnerabilities](#)
[Bulletin Archives](#)
[Viruses](#)
[Hoaxes/Phishing](#)

Policy Guidelines

[Policy on Computing](#)
[Incident Reporting](#)
[The Basics](#)
[New Users](#)
[Users](#)
[Sysadmins](#)
[Webmasters](#)
[Gridmasters](#)

Technical Info

[Security Checklist](#)
[Connectivity Checklist](#)
[Manuals and Websites](#)
[How-To Guides](#)
[Maillists and Archives](#)
[Documents](#)

Workflow

- [What is a certificate and what is it used for?](#)
- [Do I need a certificate? If so, which kind?](#)
- [How do I get one?](#) (on separate page)

Related Topics

- [Personal certificates](#)
- [Host/Service certificates](#)
- [CA certs and chain of trust](#)
- [Kerberos certificates](#)
- [DOEGrids certificates](#)
- [Kerberos vs. DOEGrids](#)
- [Certificate contents](#)
- [Storage and format](#)
- [Links to more info](#)

What is a certificate and what is it used for?

Short description:

A [certificate](#) is a mechanism used to verify an identity on a computer and/or over a computer network. You might call it a "digital identity certificate". Certificates can identify different types of entities, e.g., **persons**, **hosts** and **services**. Many restricted-access computer services are configured to identify potential users via certificates, and allow or deny access according to the certificate contents. Typical computer services that require certificate identification by users (persons) include secure web sites, grid services, and email signing and encryption. Most people only need a [personal certificate](#).

At Fermilab, most restricted services currently recognize one or both of two "brands" of certificate: the [Kerberos Certificate Authority \(KCA\)](#) is run by Fermilab and is related to Kerberos authentication. The other, the [DOEGrids Certificate Authority](#), is run by the DOE.

OS Info
Common Attack
Methods

Support and Services

Register Sysadmin
Register Node
Verify Registration
Tools
Training
Request Forms
Tlssue DB

Certificates

User Intro
Personal Certs
Host/Serv Certs
Sign/Encrypt Email
Web and SSL
Grid Use
PKI Policy
Advanced Topics

Meetings and Events

Sysadmin Round
Table


Contacts

Restricted Access

FCIRT
GCSC
MAC


At this point, you may read on, or determine [which "brand" of certificate you'll need](#), then [request it](#).

More information:

A [personal certificate](#) identifies a person, and is issued by a trusted authority (called a Certificate Authority, or CA; more on this below). The authority says: "I, being a trusted authority, certify that the person presenting this certificate is so-and-so." How does it work? The trusted authority relies on somebody it knows and trusts to verify the identity of the person requesting a certificate. Once it gets assurance of the person's identity, the authority bundles into a document known as a "certificate" the following information: a description of who the person is, who it (the authority) is, a unique identifier that it gives to the person, and an electronic signature of all of these items. Along with a certificate, the person gets a program to encrypt and decrypt information.  [Read](#)


[more about security concepts and encryption.](#)

The file containing your certificate and this device gets imported into your browser configuration. When you try to access a private or otherwise "strengthened" computer service from your browser, the certificate identifies you to the service, and, if trusted, allows you to communicate with it securely. You can also use your certificate in your email client to send and receive signed and/or encrypted email messages.

Who are the "trusted authorities"? Certificates are issued by organizations called Certificate Authorities (abbreviated as CA). There are many CAs in the world. To be eligible for a certificate from a given CA, a person needs to be affiliated with one of the organizations it handles. Furthermore, a given service recognizes certificates issued by only those CAs it has been configured to trust.  [Read about CA certificates and the chain of trust.](#)

At Fermilab, most restricted services currently recognize one or both of two CAs, (and certificates from either may pertain to any type of entity), both of which implement [Public Key Infrastructure \(PKI\)](#) based on the [X.509 standard](#). One CA, the [Kerberos Certificate Authority \(KCA\)](#) is run by Fermilab and is related to Kerberos authentication. The other, the [DOEGrids Certificate Authority](#), is run by the DOE.

Below, we discuss [personal certificates](#) and [host/service certificates](#), and what you can use them for. Most people only need a [personal certificate](#).

 For those of you who want to know more:

- [Helpful terms and concepts.](#)
- Certificates implement [Public Key Infrastructure \(PKI\)](#).
- How do [certificates relate to SSL](#)?
- Take a look at [David Youd's short, very informative cartoon intro to digital signatures and trust chains](#). It is well presented and easy to read.

At this point, you may go on to [Related Topics](#), or determine [which CA to use](#), then [request your certificate](#).

[To top of page](#)

Do I need a certificate? If so, what kind?

First of all, do you need to accomplish any of the following tasks?

- Access a restricted website (e.g., [CD Document Database](#) (certificate version), a VO Registration page, [node registration verification](#), etc.)
- Send signed email and/or exchange encrypted email
- Run grid jobs
- Administer a restricted website/web server
- Administer grid middleware on a host

If so, the answer is "yes", you need a certificate. All these tasks require a [personal certificate](#); the last two tasks require a [host/service certificate](#) in addition.

Now, which do you need: a Fermilab Kerberos or a DOEGrids personal certificate? Consult the table under [Personal Certificates](#) that lists common uses for each, to see which is better suited to your needs. You may want one of each.

To administer a web server or grid resources, also see the [DOEGrids host/service certificate table](#).

At this point, you may go on to [Related Topics](#), or [request your certificate](#).

[To top of page](#)

Personal Certificates

Certificates for people are called **personal certificates**. Most people only need this kind. Depending on what you want to do, you may need to get a Kerberos or a DOEGrids personal certificate. Most Fermilab users are eligible for both:

- To get a Kerberos certificate from Fermilab you need to have valid Kerberos credentials in the FNAL.GOV domain.
- To get a DOEGrids certificate, you must be affiliated with a DOE laboratory or project.

You may possess only one valid personal certificate at a time from a given CA. You may possess valid personal certificates from multiple CAs. You can use your personal certificate(s) in multiple applications.

The table below lists uses for Kerberos and DOEGrids personal certificates that Fermilab users are likely to encounter.

Fermilab Kerberos Personal Certificate Uses (Get one)	DOEGrids Personal Certificate Uses (Get one)
Accessing grid resources (at sites where Fermilab's KCA is trusted, e.g., for FermiGrid or OSG) FermiGrid User Installation Guide	Accessing grid resources (at sites where DOEGrids CA is trusted, e.g., for FermiGrid or OSG) FermiGrid User Installation Guide
NOT recommended for digitally signing email	Digitally signing email
Accessing some Fermilab restricted-access websites and web services (e.g., various instances of DocDB , some computer security pages)	Accessing various restricted websites and web services.
Web server admins: Setting up SSL server for Apache or IIS (need KCA personal and DOEGrids service certificates)	Web server admins: Setting up SSL server for Apache or IIS (need DOEGrids personal and service certificates)

Web authors: implementing SSL (and optionally certificate authentication) on your website	Web authors: implementing SSL (and optionally certificate authentication) on your website
Using the Nessus scanner	NOT usable for the Nessus scanner at Fermilab

[To top of page](#)

Host and Service certificates

Host and service certificates are used to authenticate hosts and services to other grid- and web-related programs, hosts and services. KCA certificates CANNOT be used for this purpose; use DOEGrids. Both ends of the connection need to trust the DOEGrids CA for authentication to succeed.

DOEGrids Host or Service Certificate Uses ([Get one](#))

Administering grid resources

[FermiGrid Administration Guide](#)

[OSG Compute Element Install Guide](#)

Administering various restricted web servers

[Apache](#), [IIS](#)

[To top of page](#)

CA Certificates and Chain of Trust

Somebody has to issue you (or your host or service) a certificate, and somebody else must decide whether to accept your certificate when you present it. This implies that there must be a "[chain of trust](#)" such that the "acceptor" trusts the "[issuer](#)". The issuer of a certificate is an organization called a Certificate Authority, abbreviated CA. A CA, it turns out, also has its own certificate, called a CA certificate (a specialized service certificate), in many cases issued to the CA by a higher-level CA. The acceptors (e.g., grid services, web services, email clients) maintain lists of issuers (CAs) that they trust.

In order to accept your certificate, the application has to find the corresponding CA certificate in its list, and that CA certificate's higher-level CA certificate if necessary, and so on, until it reaches the "root" CA certificate. Hence the chain of trust.

For optimal use of any application in which you use a personal certificate (e.g., to avoid annoying popups and possibly the occasional refusal of service), the CA's certificate should be installed in the application ahead of time to establish the trust chain. Some combinations of browser and remote site will not work unless the CA certificate chain is installed.

Notes:

- Installation of the CA certificate is not mandatory in a browser, just recommended.
- For signing/encrypting email, CA certificate installation in the email client is mandatory.
- For Windows users in the FERMI domain who use Microsoft tools (Internet Explorer, Outlook, Outlook Express), the collective domain updates take care of installing and updating the KCA CA certificate in these applications for you.

[To top of page](#)

Fermilab Kerberos Certificate Authority (KCA)

Since Fermilab has a sitewide [Kerberos](#) credential system, we are able to tie that infrastructure to PKI to create certificates for all our users. We can generate short-lived (~7 days) PKI certificates that are useful for a number of purposes, e.g., grid work and web authentication. We can also generate grid proxies from the certificates.

The system that implements this is called the "KCA" (for Kerberized Certificate Authority) and comes from work done at the University of Michigan. A KCA X.509 certificate, issued by Fermilab's KCA is tied to the user's FNAL.GOV Kerberos principal, and requires that he or she possess current, valid Kerberos credentials. The KCA certificate lifetime is typically seven days, based on the maximum renewable lifetime of Kerberos credentials. The KCA certificate must therefore be renewed frequently. Due to this short life-time, KCA certificates are not usable or not recommended for some purposes. In particular, signing or encrypting e-mail should be done with a longer-lived certificate, e.g., a [DOEGrids](#) certificate.

Unless you need a DOEGrids certificate, using KCA may be more convenient. You

avoid the trouble of registering with a CA and protecting your private key.

A KCA certificate is required by some web servers at Fermilab and assorted other applications (e.g., [Nessus](#) scanner) for which users must be [valid Fermilab computer users](#), i.e., must possess a valid, current Fermilab ID number and FNAL.GOV Kerberos principal and password.

[To top of page](#)

DOEGrids Certificate Authority

A second kind of certificate is tied to your affiliation with a DOE lab or project, is issued by the DOE's CA, called [DOEGrids](#). Fermilab computer services that require public key certificates but that are open to a wider audience than just Fermilab people typically recognize the DOEGrids CA. In addition, a DOEGrids certificate is required for [DOE-related grid computing](#), for access to many restricted web sites related to DOE labs and/or projects, and may be used to digitally sign outgoing email.

DOEGrids also issues [host/service certificates](#).

Kerberos vs. DOEGrids Personal Certificates

- Both "brands" of certificates, Kerberos and DOEGrids, are based on PKI and are in X.509 format.
- Kerberos certificates are available only for holders of Fermilab Kerberos principals (with currently valid Kerberos password). DOEGrids certificates are available to people associated with DOE-funded projects and laboratories.
- Kerberos authenticates on the basis of your FNAL.GOV Kerberos credentials. DOEGrids authenticates based on a DOE affiliation and your sponsor's knowledge of your identity, obtained from having met you in person.
- KCA issues only personal certificates. DOEGrids CA issues both personal and host/service certificates.
- A Kerberos certificate lasts only as long as the maximum renewable lifetime of your Kerberos credentials (seven days). A DOEGrids personal certificate lasts one year.
- The uses for the two "brands" of personal certificates are listed in the [table above](#).

[To top of page](#)

What information is in a PKI X.509 certificate?

The specific fields included in a certificate varies from CA to CA. Here is a list of information that is included in virtually all personal certificates; it is not an exhaustive list:

- Subject of the certificate (the person or other entity to whom it was issued)
- Subject's public key
- Issuer (the Certificate Authority)
- Serial number (an integer that is unique to all certificates signed by the CA that issued this certificate)
- Extensions (subject's email address, subject type, policy information, etc.)
- Validity Period (start and end dates)
- Signature algorithm (the name of the algorithm used for signing; this is used to test for tampering)
- Netscape Cert Type (e.g., SSL client, SSL server, S/MIME, etc.)
- Key usage (what uses can the certificate be applied to)

[To top of page](#)

The certificate store and file format

When your certificate is imported into a browser, it gets put in a location called a "certificate store", where the browser can access it. Depending on your OS, your browser and your email client, your email client may be able to access the certificate from the same certificate store. There's no need to import your certificate into more than one of the applications that share a store. The following pairs of applications share a store:

- Microsoft Internet Explorer and Outlook (or Outlook Express)
- Mozilla browser and email client
- Netscape browser and email client
- Macintosh native email clients and browsers use the keychain files

Firefox and Thunderbird do not share a store.

The file formats are:

- .pfx
PKCS#12 format binary file on Windows, multi-part, contains certificate and private key
- .p12
PKCS#12 format binary file on Unix/Linux/Windows, multi-part, contains certificate and private key
- .key
often a binary file containing a private key
- .pem
a Base-64 encoded file which may be a private key or an X.509 certificate, or some combination.
- .cer and .crt
binary format certificate file
- .cert
certificate in either binary format or, more usually, text dump of certificate

Browsers require a binary certificate format called PKCS#12 whereas grid software, Globus in particular, uses PEM format. KCA and DOEGrids issue certificates in PKCS#12 format. The PKCS#12 file contains both your certificate and your (encrypted) private key. The file extension is typically p12 if obtained through a browser on UNIX and pfx on Windows. If you plan to use grid software, you'll need to convert the format to PEM; instructions are specific to the CA: see [KCA](#) or [DOEGrids](#).

Within your certificate, you are identified uniquely by your "distinguished name" or DN. A DN has several components which identify the issuing CA, your organization, you (and possibly other entities).

The [KCA certificate format has Subject DNs](#) of the form:

```
/DC=gov/DC=fnal/O=Fermilab/OU=People/CN=<your name> /UID=<your_principal>
```

e.g.,

```
/DC=gov/DC=fnal/O=Fermilab/OU=People/CN=Joe Blow /UID=<joeblow>
```

The DOEGrids certificate format has Subject DNs of the form:

```
/DC = org/DC = doegrids/OU = People/ CN = <your name> <some 6-digit number>
```

e.g.,

```
/DC = org/DC = doegrids/OU = People/ CN = Joe Blow 123456
```

[To top of page](#)



Links to more information:

- [David Youd's short, very informative cartoon intro to digital signatures and trust chains](#)
- [Everything you Never Wanted to Know about PKI but were Forced to Find Out](#) (Peter Gutmann, U of Auckland). (PDF format) You don't actually need to know it all, but it's there if you're curious!
- The [Globus Toolkit 4.0 Security Glossary](#) defines many terms that pertain to certificates.
- [Overview of Grid Computing](#) (Fermilab)
- [VOMRS v1_2 manual](#), Chapter 3 (Fermilab)
- http://www.nordugrid.org/documents/certificate_howto.html
- http://en.wikipedia.org/wiki/Public_key_certificate
- http://www.dartmouth.edu/~pkilab/pages/Using_PKI.html
- http://www.dartmouth.edu/~pkilab/pages/Using_SMIME_e-mail.html
- <http://www.marknoble.com/tutorial/smime/smime.aspx>
- <http://www.tldp.org/HOWTO/SSL-Certificates-HOWTO/>
- <http://computer.howstuffworks.com/encryption.htm>

Workflow

- [What is a certificate and what is it used for?](#)
- [Do I need a certificate? If so, which kind?](#)
- [How do I get one?](#) (on separate page)

Related Topics

- [Personal certificates](#)
- [Host/Service certificates](#)
- [CA certs and chain of trust](#)
- [Kerberos certificates](#)
- [DOEGrids certificates](#)
- [Kerberos vs. DOEGrids](#)
- [Certificate contents](#)
- [Storage and format](#)
- [Links to more info](#)

For assistance contact helpdesk@fnal.gov.

Information compiled and maintained by [Computer Security Team](#) ; last modified by TR on July 13, 2006.

(Address comments about page to the [Computer Security Team](#).)

[Security, Privacy, Legal](#)
[Fermilab Policy on Computing](#)

 Fermi National Accelerator Laboratory