

CACert and Single Sign On

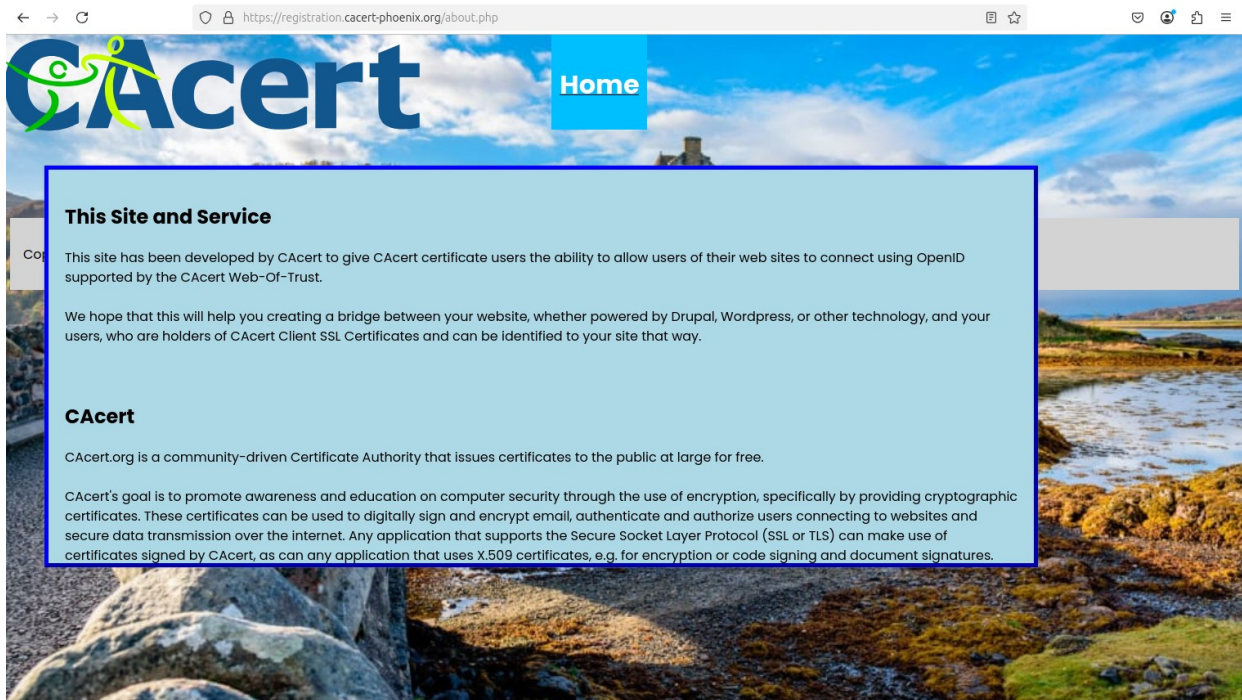
CACert has developed a method of using your CACert Client Certificate to facilitate easily signing in to web sites and other on-line resources. This uses the OpenID Connect standard, which is commonly used around the world.

This facility can be used by doing the following:

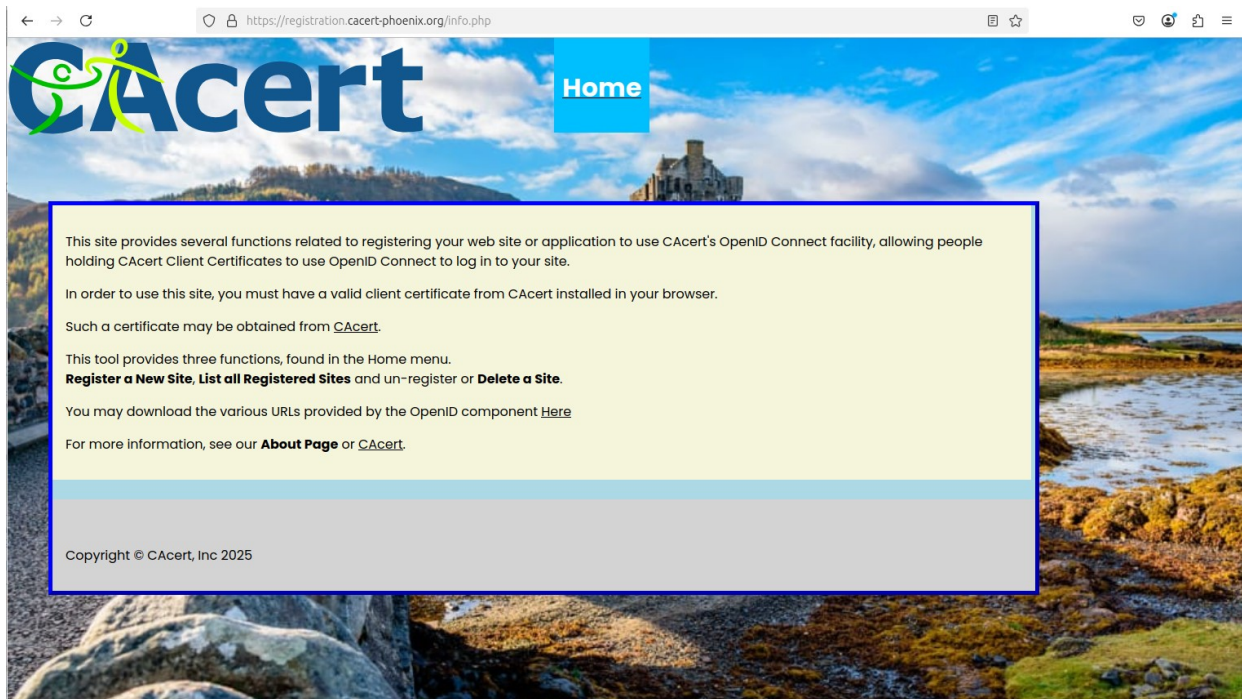
1. Go to <https://registration.cacert-phoenix.org/index.php>, the site to register your Client Certificate and the on-line resource that you wish to use.



2. The About Page, <https://registration.cacert-phoenix.org/about.php>, gives some background information about the site and its history.

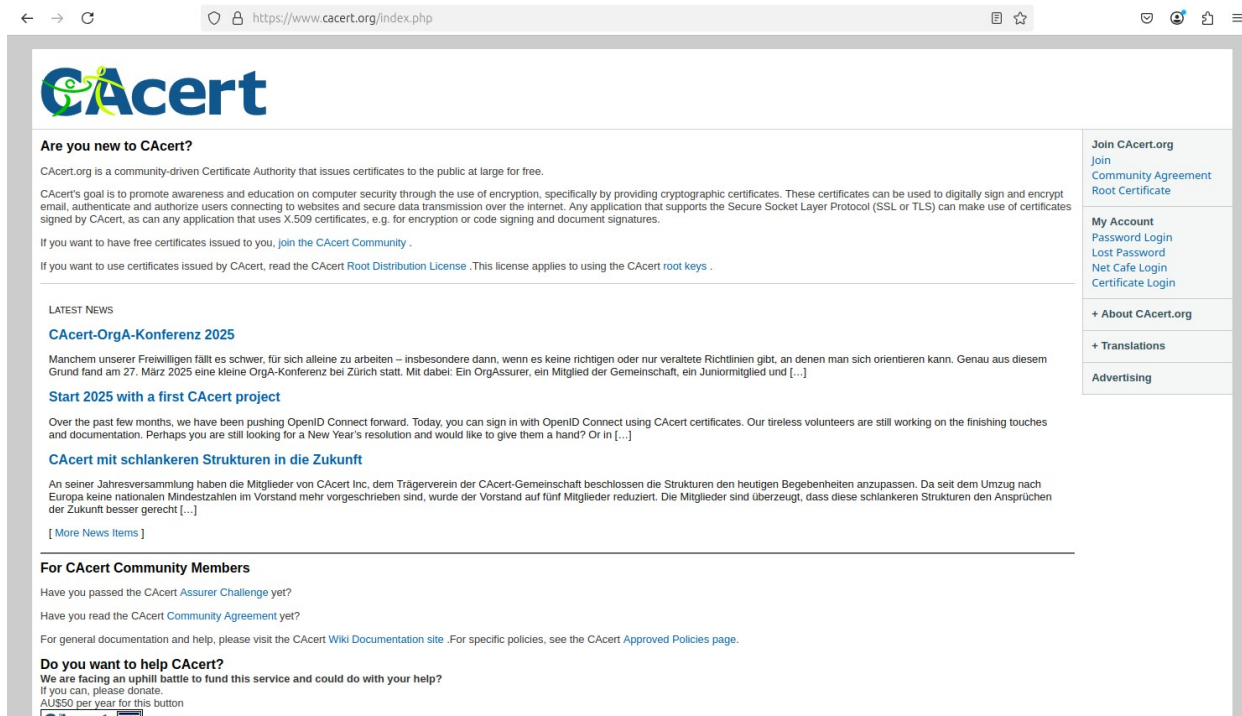


3. The Info Page, <https://registration.cacert-phoenix.org/info.php>, gives a very basic overview of the facilities provided by the site.



CAcert Client Certificates


1. Before using this facility, you will need a CAcert Client Certificate, which can be obtained from <https://cacert.org>. You must be a member of CAcert, which can easily be done from that page.



The screenshot shows the CAcert.org website. At the top is the CAcert logo. Below it, a section titled "Are you new to CAcert?" explains that CAcert.org is a community-driven Certificate Authority. It mentions that CAcert's goal is to promote awareness and education on computer security through encryption. It also states that CAcert issues certificates to the public at large for free. A link to "Join the CAcert Community" is provided. Below this, a section titled "LATEST NEWS" features three articles: "CAcert-OrgA-Konferenz 2025", "Start 2025 with a first CAcert project", and "CAcert mit schlankeren Strukturen in die Zukunft". To the right of the main content is a sidebar with links for "Join CAcert.org", "My Account", "+ About CAcert.org", "+ Translations", and "Advertising". At the bottom, there is a section for "For CAcert Community Members" with links to "Have you passed the CAcert Assurer Challenge yet?", "Have you read the CAcert Community Agreement yet?", and "Do you want to help CAcert?".

2. If you use multiple e-mail addresses to log in to different web sites and services, you should create a certificate that includes all of those e-mail addresses. In most browsers, changing the certificate that is remembered by the browser can be a bit difficult.
3. The procedure for obtaining a valid Client Certificate can be found at <https://community.cacert.org/clientcert>

← → ↻ <https://community.cacert.org/clientcert/> ☆



Client certificate generation in your browser

Start

1. Generate a key pair

Your name

Please input your name as it should be added to your certificate

Choose an RSA key size

An RSA key pair will be generated in your browser. Longer key sizes provide better security but take longer to generate.

☒ 3072 Bit

☐ 2048 Bit (most compatible, least secure)

☐ 4096 Bit

Generate key pair and signing request

© 2023 CAcert

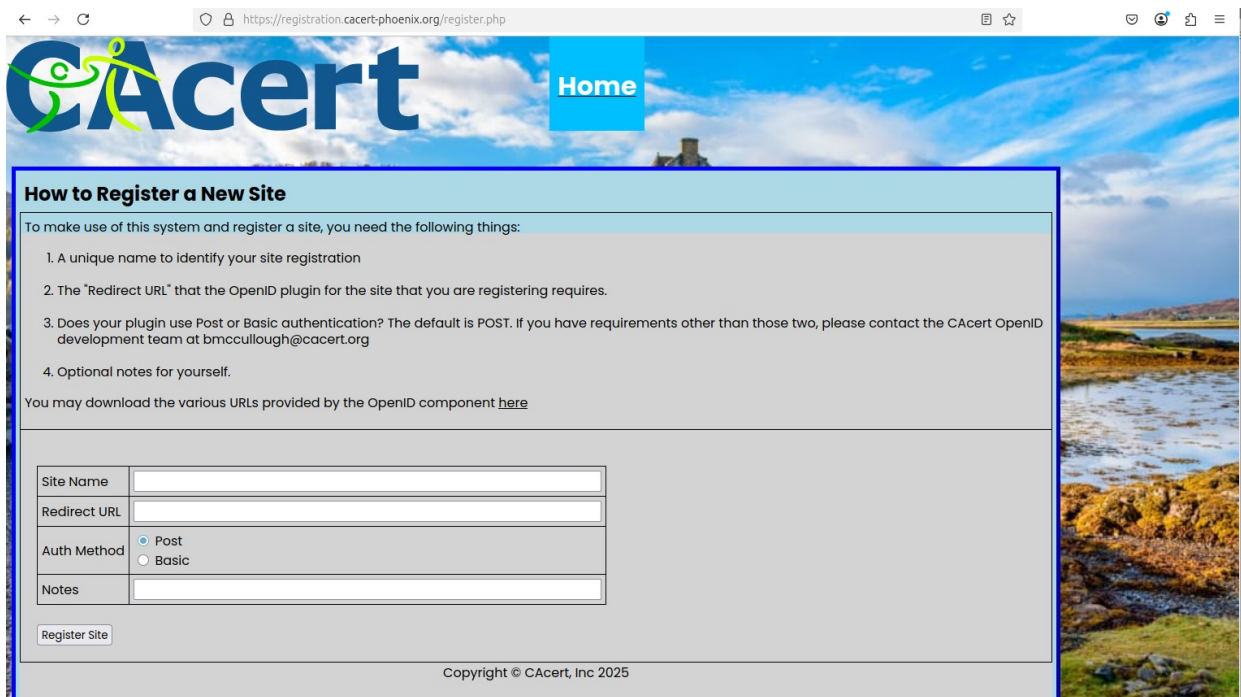
CAcert OpenID Connect Registration

1. Once you have your CAcert Client Certificate, go to the CAcert OpenID Registration site: <https://registration.cacert-phoenix.org/index.php>
2. I will be using NextCloud as our example of a site to register. Other alternatives are shown in a related set of documents listed under. **“CAcert OpenID Connect Registration Examples”**
3. To register a new site or on-line resource, you will need a few pieces of information and **MUST** record the answers given by this tool. They will not be available after you have finished the process.
4. The information that you will need is:
 1. The Site Name (for your own reference) -- This can be any string of characters and is purely for your own information
 2. The Redirect URL that the on-line resource provides to you.
 3. Whether this site requires POST or Basic (GET) connections. Most use POST.
 4. You may also record some notes for yourself.
 5. The tool will provide you with two values, Client ID and a Client Secret. They **MUST** be recorded by you outside of the tool, because you will not be able to retrieve them after this process is complete.
5. Note: The on-line resource that you wish to connect to will require one of two access methods. The first uses the tool as provided, but some require a JSON structure to be

provided. That can be downloaded here: <https://registration.cacert-phoenix.org:4444/.well-known/openid-configuration>

6. Once you have collected the required information, you can proceed with registering that on-line resource.

7. First, go to the Register A New Site page on the web site. <https://registration.cacert-phoenix.org/register.php>

A screenshot of a web browser showing the CACert registration page. The browser's address bar displays 'https://registration.cacert-phoenix.org/register.php'. The page features the CACert logo on the left and a 'Home' button on the right, both set against a background image of a coastal landscape with a lighthouse. The main content area is titled 'How to Register a New Site' and lists four requirements for registration. Below the list is a form with fields for 'Site Name', 'Redirect URL', 'Auth Method' (with radio buttons for 'Post' and 'Basic'), and 'Notes'. A 'Register Site' button is located at the bottom of the form. The footer of the page contains the text 'Copyright © CACert, Inc 2025'.

8. To Be Continued