How do I support SSL Client Certificate authentication?

Asked 16 years, 3 months ago Modified 12 years, 1 month ago

Viewed 15k times

12

I want to do what myopenid does -- once you've logged, you can click a button that generates you an SSL certificate; the browser then downloads this certificate and stores it. When you later go back to yourid.myopenid.com, your browser can use its stored certificate for authentication so you don't ever need a password.

So my questions is what is required to get this working? How do I generate certificates? How do I validate them once they're presented back to me?

My stack is Rails on Apache using Passenger, but I'm not too particular.

ruby-on-rails **apache** **ssl**

Share

Improve this question

Follow

asked Aug 26, 2008 at 16:57

James A. Rosen

65.2k ● 62 ● 184 ● 263

5 Answers

Sorted by: Highest score (default)

8

✓

These are usually referred to as client side certificates.

I've not actually used it but a modified version of restful-authentication can be found here [here] that looks like what your after.

I found this via [Dr. Nic's post]

Share Improve this answer Follow

answered Aug 26, 2008 at 17:51

russtbarnacle

915 ● 1 ● 10 ● 14

2

Depends on the server, but the simplest solution I know of, using Apache:

[FakeBasicAuth]

> "When this option is enabled, the Subject Distinguished Name (DN) of the Client X509 Certificate is translated into a HTTP Basic Authorization username. This means that the standard Apache authentication methods can be used for access control. The user name is just the Subject of the Client's X509 Certificate (can be determined by running OpenSSL's openssl x509 command: openssl x509 -noout -subject -in certificate.crt). Note that no password is obtained from the user... "

Not sure about rails, but the usual REMOTE_USER environment variable should be accessible in some way.

Share Improve this answer Follow

answered Aug 26, 2008 at 18:01

Mark Renouf
31k ● 19 ● 96 ● 125

1

If you want to generate certificates, you need to cause the client to generate a key pair, and send you at least the public key. You can do this in Firefox via a Javascript call, it's crypto.generateCRMFRequest. I'm guessing there are browser-specific methods available in other browsers too. But first, you need to figure out how to issue a certificate once you get a public key.

You could script something on the server with OpenSSL, but it has built-in support for CSRs, not the CRMF format Firefox will send you. So you'd need to write some code to convert the CRMF to a CSR, which will require some sort of DER processing capability… I'm just scratching the surface here—operating a CA, even for a toy application, is not trivial.

SSO solutions like OpenId and PKI solutions do overlap, and there is an elegance in PKI. But the devil is in the details, and there are good reasons why this approach has been around a long time but has only taken off in government and military applications.

If you are interested in pursuing this, follow up with some questions specific to the platform you would want to develop your CA service on.

Share Improve this answer

Follow

answered Aug 28, 2008 at 20:39

erickson

269k ● 59 ● 401 ● 497

You could just use the keygen element instead, whatwg.org/specs/web-apps/current-work/multipage/… – hendry May 26, 2009 at 7:55

▲

1

▼

You can generate a certificate in the client's browser using browser-specific code. See this question

You could also generate SSL client certs server-side using OpenSSL in Ruby (see this q). (This will work in any browser without browser-specific code, but your server will have generated the client's private key, which is not ideal for crypto purists.)

Whichever method you use to generate them, you will then need to configure your webserver to require the client certificates. See the Apache docs for an example.

Share Improve this answer

Follow

edited May 23, 2017 at 12:10

Community Bot

1 ● 1

answered Oct 29, 2012 at 14:49

Rich

15.4k ● 3 ● 71 ● 123

CSR generation (or equivalent) works in most popular browsers (IE, FF, Chrome, ...), but the code tends to be browser-specific. See this answer: stackoverflow.com/a/9198400/372643 – Bruno Oct 29, 2012 at 15:12

Great answer, Bruno - I think that's a better answer to this q than any currently on here :-) – Rich Oct 30, 2012 at 17:16

0

I've been working on a solution to this problem. I wanted to do the same thing and I know lots of other website owners want this feature, with or without a third party provider.

I created the necessary server setup and a firefox plugin to handle the certificate-based authentication. Go to mypassfree.com to grab the free firefox plugin. Email me (link on that page) for the server setup as I haven't packaged it yet with a nice installer.

Server setup is Apache2 + OpenSSL + Perl (but you could rewrite the perl scripts in any language)

Jonathan

Share Improve this answer Follow

answered Jan 9, 2009 at 19:58

apricoti