Firefox prompts multiple times to select my personal certificate

Firefox prompts multiple times to select my personal certificate

Question

For some sites, such as the eCAT landing page (http://web.mit.edu/ecat/ecat3), or the HR forms site (http://web.mit.edu/hr/forms/academic.html) Firefox prompts multiple times for me to select which personal certificate to use. How can I resolve this?

Answer 1

The default configuration in Firefox is to "Ask every time" which certificate you'd like to use. This setting is problematic for some websites, and Firefox will ask multiple times, even if you have only one personal certificate installed.

For the purpose of avoiding this behavior, you can configure Firefox to select your certificate automatically, instead of prompting you to choose one. To do this:

1. Follow the menu path **Tools > Options (Windows) or Firefox > Preferences (Mac)**.
2. Navigate to the **Privacy & Security** tab.
3. Scroll down the page to the **Certificates** section.
4. In the **Certificates** section, where it says "When a server requests your personal certificate", select **Select one automatically**.

For security reasons, and depending on whether the computer is solely for your own use, it may be better to change the setting back to Ask Every Time once you have finished accessing the site.

Note: For users who do not wish to change the setting to Select One Automatically, the multiple prompts do not seem to occur in Firefox 3.5 or later. For more, see: https://stackoverflow.com/a/72971260.

More information

The following information does not directly pertain to this article, but may be useful for informational purposes.

This pertains to Firefox displaying the site after just one prompt for the certificate, then prompting for at regular intervals with pauses in between, for as user is viewing the site.

When an SSL client and an SSL server go through the full procedure of negotiating a cryptographic connection (known as a "handshake"), including any authentication, they establish a "session". The client and server are each supposed to keep the information about that session in a local store (or "cache") of sessions (typically kept in RAM memory), and to reuse it in subsequent connections, rather than going through the full handshake again every time. That session is expected to last in the cache until:

1. Either the client or server is stopped (or restarted),
2. The client or server operator manually empties the cache,
   or
3. The cryptographic device (if one is being used) is disconnected, or
4. Some time limit has expired. The recommended time limit is 24 hours, although it's common to use 8 hour limits.

The intended effect is that a user needs to authenticate to each server only once a day, or as often as he restarts his browser, which ever comes first.

On an apache web server, the configuration setting to take a look at is SSLSessionCacheTimeout.