

# Re: standalone CA customized certificate

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2007-03/msg00029.html>

---

- *From:* Brian Komar [MVP] <[bkomar@xxxxxxxxxxxxxxxxxxxxxx](mailto:bkomar@xxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 20 Mar 2007 13:07:52 -0400
- 

In article <2D8A7466-07B7-4601-844D-3FE805F2ABE0@microsoft.com>, SunilVirmani@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx says...

Hi Brain,

It is regarding the following

Further I want to add serial number and processor type of my terminal machines in the certicate.

My understanding is that when we issue a client certificate on the basis of email address , we embed the email address in the certificate.Now each of my client machine will be distinguished by serial number and processor type. Should not i put the serial number and processor type in the certificate.

Please let me know if my understanding is incorrect . Further What kind of information (instead of email address) should be in the certificate to distinguish the two certificate.

Regards,  
Sunil

<snip>

You are definitely making some assumptions. Client authentication certificates require two things:

- 1) The client authentication OID in the EKU or application policy extension (or both). This states that the certificate is for authentication purposes. In addition, the purpose of the certificate must be for digital signature.
- 2) The subject must contain a subject that is recognized by the authenticating server. For most MS apps, the subject name for is the User Principal Name (UPN) stored

Re: standalone CA customized certificate

in the subject alternate name. Alternatively, you can use some applications to map a certificate subject name format to a specific account. This is where you could use email name, or any other form of distinguished name. I have seen some custom applications where a subject alternate name was used to look up an account (GUID in their case) against a SQL or Oracle database.

If you are wanting to put processor type or serial number, what application are you using/coding that would look up this information. You are trying to mix machine specific information into a user authentication certificate by the looks of it.

The question comes down to: What application are you trying to secure with these authentication certificates?

Brian

.