72nd IETF Kerberos Working Group

draft-ietf-krb-wg-anon-05.txt
Last Call Issues
With anonymous PKINIT, what should the client realm be?

PROPOSAL

When anonymous PKINIT is used, the returned realm name MUST be the anonymous realm.
Draft -05 said the KDC MAY remove AD-INITIAL-VERIFIED-CAS subject to policy.

Draft -07 says it SHOULD do so.

Is this change OK?
How should anonymous realms interact with cross-realm policy?
In the anonymous AS request, which KDC do you contact for the anonymous ticket?
A022 - Is anonymous@REALM anonymous?
Ken Raeburn <raeburn@mit.edu>:

- WELLKNOWN/ANONYMOUS@REALM gives the server some information about the identity of the client.

- Should this be treated as anonymous at the GSS-API layer?
Should importing an anonymous Kerberos principal name and calling display_name get NT-ANONYMOUS back as the type? or

Should NT-ANONYMOUS names only be generated by accept_sec_context?
If I call gss_display_name on an anonymous principal in an acceptor, what do I expect to get back?