Advisory: Use at least SHA-1 for RADIUS server certificates (Apr 2014)

Buried in the historic mail archives (and likely in some older eduroam documentation) are advisories concerning the type of RADIUS certificate that eduroam(UK) participants should be using. Basically, do not use MD5 certificates.

For some time now, MD5 has been deprecated and over the past few years Operating Systems have been dropping support for such certificates.

e.g. http://support.apple.com/kb/HT4999 [1] (since iOS 5 MD5 certs are only valid for CA certs not server certs)

Android and Chromium have also been mooting the move of stopping MD5 support e.g.

http://dev.chromium.org/developers/md5-certificate-statistics [2]

Note that whilst there hasn't been much information regarding larger SHA-x support on clients (eg SHA-256 or SHA-512) there has not been any noted issues with SHA-1 usage

Summary. Your RADIUS server should be using at least a SHA-1 certificate (root may still, currently, be MD5 but strongly advised to also be SHA-1)

Links
[1] http://support.apple.com/kb/HT4999
[2] http://dev.chromium.org/developers/md5-certificate-statistics