Advisory: Windows Mobile 8 and certificate verification (Apr 2014)

Announcement regarding Windows Mobile 8 and 802.1X authentication with certificate validation

Best practice is that clients must be configured to trust/verify the CA that signs the RADIUS server that presents during an 802.1X authentication - a major security pin for eduroam is this trust/check.

It has been noted that Windows Mobile 8 (WM8) devices would not authenticate the user if this 'verify' option was chosen.

Research undertaken within GEANT members, the UK 802.1X SIG and verified by eduroam UK
support is that this is due to WM8 requiring an extra attribute in the RADIUS server cert (note, we have verified that successful authentication can occur if ONLY the RADIUS server cert has this attribute present). The attribute is the Certificate Revocation List (CRL) Distribution Point (CDP) e.g.

crlDistributionPoints = URI:http://www.example.ac.uk/example.crl [1]

For Windows Mobile 8 to have proper/safe 802.1X authentication your RADIUS servers will need to have such an attribute present - we are just awaiting feedback/confirmation as to whether things work if only the CA cert has this attribute (not something that we can test in the short term)

Alan

Links
[1] http://www.example.ac.uk/example.crl