Advisory: Impact of change of Certificate Service CA on eduroam Home service providers

January 2016 - 20/01/2016

This advisory is relevant to all eduroam(UK) Home (IdP) service organisations that are using server certificates supplied through the Jisc Certificate Service (Janet Certificate Service) for RADIUS servers acting as authenticators. It describes the effect of the change to the new certificate authority which occurred in May 2015, together with the measures that need to be planned for and put into effect.

Originator: Edward Wincott

Background and Scope

The certificate authority (CA) which issues server certificates provided through the Jisc Certificate Service (Janet Certificate Service/JCS) changed from Comodo to QuoVadis on 12/05/15. This resulted from the move away from the TERENA service, which co-incidentally also changed its CA in early 2015, to a directly procured Jisc service. The switch to QuoVadis enables Jisc to provide an even better value service as well as allowing operational improvements. However, the change of CA has implications for all eduroam organisations using EAP methods that utilise CA certificates (effectively all) and whose authenticating RADIUS servers' certificates have been supplied through the Jisc Certificate Service. This advisory relates to the changes to client supplicant configuration necessitated by the change of CA. ***Organisations which use their own self-signed certificates on authenticating RADIUS servers are not affected.***

Unless the certificate expiry date of your certificate is imminent, no immediate is necessary for existing Comodo based certificate installations. Certificates are typically issued for 2 or 3 years and current deployments can remain as they are until expiry dates approach. When Comodo certificates do expire they will have to be replaced. Replacement certificates issued through the Janet Certificate Service will be from QuoVadis.

Potential Problem

Properly setup client devices should validate the CA of the certificate installed on authenticating RADIUS servers (and should also check the common name (CN) defined on the certificate) during the TLS handshake phase. Unless the configuration of the supplicant on users' devices is modified and in some cases the certificates stores too, replacing the expired certificate of the RADIUS server with one signed by a different CA will cause *properly set up client devices* to fail to authenticate.

Actions to be taken

Before an organisation using Comodo server certificates issued by the Jisc Certificate Service for its authenticating RADIUS servers renews these with QuoVadis certificates, it must take certain measures to ensure the continuance of successful authentication of its users' devices with the minimum of disruption.

Essentially, the configurations of all client devices will have to be updated. The method chosen and the timing of this depend on the mechanism by which users' devices are configured at your organisation.

The following need to be achieved:

- QuoVadis root and intermediate certificates must be in the client certificate store (specifically QuoVadis Root CA 2, QuoVadis EV SSL ICA G1 and/or QuoVadis Global SSL ICA G2 depending on the type of certificate you have purchased, see https://www.quovadisglobal.com/sslbundle.aspx [1])
- The QuoVadis CA 2 root must be trusted by the supplicant
- The CN defined on the authenticating RADIUS servers' certificate must be configured in the supplicant (this should not change unless you are changing your chosen CN on the certificate)
- The new QuoVadis server certificate needs to be installed on the authenticating RADIUS server(s) together with its associated private key file and the relevant EAP module needs to be configured to use it.

Notes

Regarding CA certificates in client device cert stores - most manually configured machines will already have these and so reconfiguration should be a straightforward matter of simply changing the CA in the Trusted Root Certification Authority selection panel of the Wi-Fi supplicant (see screen shot in Appendix). ***If you support manual configuration of clients and have produced manual configuration instructions, these will need to be updated and your user base advised of the changed instructions.***

CAT configured machines - all parts of the certificate required to validate the certificate by the client must be uploaded to CAT; ie root, intermediates and server certificate for assured compatibility. Root and intermediates is the minimum. Best practice recommendation is that intermediates only is not sufficient since less well known CAs may not be distributed with the OS or otherwise have been saved in the client cert store. (This certainly applies if you are using self-signed/private certificates!) Similar considerations will apply to other automated client setup tools. ***You will need to make the requisite changes to CAT and advise your user base to re-run the eduroam installer.***

If you are running multiple authenticating RADIUS servers, for simplicity we recommend that you use the same certificate for all servers. This will of course also require the private key file to be copied to all servers sharing the certificate. Whilst you can use separate certificates for each server, using just one simplifies client configuration since it means that only one CN

need be defined in the ‘connect to these servers’ box.

Whilst this advisory applies to organisations using the Jisc Certificate Service, which provides highly cost effective server certificates from a CA whose certs are widely distributed in clients, it remains best practice for organisations to use self-signed certificates. The benefits of setting up as your own CA are security, performance, control and I you utilise EAP-TLS, client certificates can readily be produced. The downsides are: operating your own CA and distributing certificates (but that’s only a small issue these days with on-boarding tools such as CAT).

Recommended reading: EAP Server Certificate guidance on the eduroam.org wiki can be found at:

https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-Consideration2:Recommendedcertificateproperties [2]

Appendix

Windows 7 PEAP Properties Screenshot

Manually configured clients should already have the public QuoVadis CA certificates in their certificate stores, so reconfiguration should be a straightforward matter of simply changing the CA in the Trusted Root Certification Authorities selection panel in the PEAP Settings config box.

For PEAP (for CN=radius.camford.ac.uk on certificate):

Links
[1] https://www.quovadisglobal.com/sslbundle.aspx
[2] https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-Consideration2:Recommendedcertificateproperties