Published on *Jisc community* (https://community-stg.jisc.ac.uk)

2020-07 Advisory: EAP server certificate considerations

eduroam(UK) Advisory: EAP server certificate considerations (July 2020)

This advisory is relevant to all eduroam(UK) Home (IdP) service organisations. It describes the evolving requirements applying to RADIUS server certificates used in eduroam as the result of measures taken by commercial certificate authorities, web browser and operating system vendors. The measures include changing the maximum period of validity of server certs supported in client root cert stores together with changes to Apple OSs requirements relating to security sensitive parameters in server certs.

The implications of the changes being introduced are described together with recommendations for member organisations, both those operating their own CAs and those who purchase certificates from commercial vendors, including the Jisc Certificate Service. No action is needed immediately since current RADIUS server certificates will continue to support eduroam until they expire. But you should understand how the requirements will affect the configuration of your server certificates when you next renew them – there is an impact on length of validity, CN and SAN entries, CRL URL and signing algorithm.

Nb. If you use a certificate from a commercial CA, after 31 August the maximum length of validity will be 398 days. So if your certificate expires before December 2020, you might want to consider renewing it early, before the end of August so that you can take advantage of a longer period of validity (825-days).

9th July 2020

Introduction

eduroam uses the EAP family of protocols in RADIUS for authentication. EAP protocols use encryption to safeguard the contents of the protocol conversation; most EAP protocols (other than EAP-PWD) rely on the X.509 standard which defines public key certificates. X.509 is also used by the TLS and SSL protocols, which form the basis of HTTPS. There have been multiple developments that will impact the deployment of these X.509 certificates, and by extension, your eduroam home service.

A time line

In March 2017, the CA/Browser Forum, an industry body made up of commercial certificate authorities, web browser and operating system vendors, passed a resolution to limit the length of validity of X.509 SSL/TLS certificates to 825 days. Prior to this change, maximum validity

for Domain- and Organisation Validated certificates was 39 months, and Extended Validation certificates were capped at 27 months. This change came into force on 1 March 2018.

In September 2019, the CA/Browser Forum voted on a proposal, SC22, to reduce certificate validity length even further. The proposal failed due to a lack of quorum, but the vote to pass the proposal was unanimous amongst the browser and operating system vendors. Apple issued a notice in November 2019 (https://support.apple.com/en-us/HT210176 [1]) to inform app developers and service providers that its operating systems would be strict in enforcing the validity requirements agreed in 2017 starting with iOS 13 and macOS 10.15.

Further to the vote in September 2019, Apple, Mozilla and others opted to enforce the issue of the SC22 proposal in their products, starting on 1 September 2020. Apple issued updated advice in March 2020 (https://support.apple.com/en-us/HT211025 [2]) that limits the length of validity of certificates issued by CAs that Apple includes in its operating systems to 398 days (effectively 13 months). This advice does *__not__* apply to private certificate authorities, such as recommended by eduroam. Mozilla followed in July 2020 with its own advice here: https://blog.mozilla.org/security/2020/07/09/reducing-tls-certificate-lifespans-to-398-days/ [3]

Implications for eduroam

In November 2019, after Apple issued its notice, the eduroam SG issued updated advice on EAP server certificate considerations here (particularly Consideration 2):

https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations [4]

Following the information by Apple in March 2020, we recommend that all our eduroam members review these considerations in light of these developments:

1. If you have chosen to have your EAP server certificate issued by a commercial certificate authority (including the Jisc Certificate Service), you may continue to use the existing certificate until it expires. Thereafter, you must use a server certificate that is not valid for more than 398 days. If your certificate expires soon, you may wish to have your certificate reissued before 31 August 2020 and extend your service’s lifetime with 825-day validity.

2. If you have chosen to have your EAP server certificate issued by your own certificate authority (the default for users of the Microsoft NPS server), you may continue to use the existing certificate you issued until it expires. Thereafter, you should issue server certificates that are not valid for more than 825 days. Additionally, to ensure continued functionality on Apple and Windows devices, you must also comply with the following:

    - Discontinue the use of SHA-1 as the signature algorithm; use SHA-256 or SHA-512 instead.
    - Discontinue the use of the CommonName (CN) for presentation of the DNS name of the server; use the Subject Alternative Name (subjectAltName) instead.
    - Ensure that the Certificate Revocation List is accessible externally via HTTP and is correctly set in the CRL Distribution Point extension of your CA root certificate.

3. Regardless of type of certificate authority, the eduroam SG recommendation of a key length of at least 3072 bits is still applicable.

Additional information

Let’s Encrypt issues certificates that expire after 90 days. An example of how to use Let’s Encrypt certificates with FreeRADIUS can be found here: https://framebyframewifi.net/2017/01/29/use-lets-encrypt-certificates-with-freeradius/ [5]

Source URL: https://community-stg.jisc.ac.uk/library/network-and-technology-service-docs/2020-07-advisory-eap-server-certificate-considerations

Links
[1] https://support.apple.com/en-us/HT210176
[2] https://support.apple.com/en-us/HT211025
[3] https://blog.mozilla.org/security/2020/07/09/reducing-tls-certificate-lifespans-to-398-days/
[4] https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations
[5] https://framebyframewifi.net/2017/01/29/use-lets-encrypt-certificates-with-freeradius/