2021-04 Advisory: Android 11 configuration issues, geteduroam, server certificates

Released 1st April 2021

Updated 16th April 2021

This advisory applies to all organisations providing a Home (IdP) service who wish to support users on Android 11 devices. A number of issues have arisen simultaneously which have resulted in a complex situation which requires a careful response from member organisations to avoid user disappointment.

The recommended actions are summarised at the bottom of this page.

Contents:

Background

The latest version of Android no longer gives users the option of disabling validation of the server certificate presented during EAP authentication. This implements best security practice and is a requirement of the WPA3 standard which will be adopted in the future by all operating system developers. This has however led to difficulties for some users, since organisations which operate their own certification authority now need to find a solution to distributing their root certificate to user devices and getting the devices properly set up to check the certificate. To add to this, there are currently problems specific to certain device manufacturers relating to their implementation of Android 11. These relate to particular aspects of the most popular EAP methods used by organisations whose authentication systems are based the 802.1X standard (ie eduroam members). A third strand to the problem is that the new geteduroam user device configuration tool implements the expectation of eduroam developers that subjectAltName be used as the naming method by sys admins for their server certificates.

The European GEANT eduroam confederation developed the eduroam CAT tool (the ‘CAT tool’) many years ago specifically to make setup of user devices problem free. This relies on the member organisation setting up a profile correctly for its users to download and this has been very successful with Windows, Apple and Linux devices – all that is needed is for the user to get the configuration profile and the executable installer from the cat.eduroam.org website. On Windows, users simply needed to download and run the installer, effectively one operation; on Apple and Linux systems, all that was needed was the profile configuration file.

For Android, the process was more complex in that a separate Android App was required to actually run the installation – the eduroam CAT App (the ‘CAT App’) from the Google Play store.

A number of our counterpart NRENs in Europe, originally with the objective of adding support for additional authentication methods (EAP-TLS), have developed the geteduroam App. Because the CAT App was no longer in active development and crucially, with new APIs being utilised in Android 11 and Google’s requirements for inclusion in the Google Play store precluding updates to the old App, geteduroam now supercedes the old CAT App for Android 11 and beyond. This has meant that we have had to adopt geteduroam perhaps sooner in its development cycle than ideal. But the great benefit of geteduroam is that it continues to work with the CAT tool and allows the download of the profile and installation to be carried out in one operation on Android, Apple’s mobile OSes and Windows Mobile. The future is promising once further development work by GEANT/the NRENS involved has progressed and bugs in early versions of Android have been resolved.

geteduroam

Since geteduroam is very new, there are at present certain issues. geteduroam has been developed for Android 11 and uses the latest Android 11 APIs, therefore it is only recommended for use with Android 11 devices.

The certificate naming constraint that geteduroam implements on server certificates for several EAP types (including PEAP) is that the certificate name must be in both the CN and subjectAltName:DNS fields. This is not a problem with public CA issued certificates, since most fill the subjectAltName by default. But we have noticed that some private CA certs have omitted entering the certificate name in this field. The eduroam recommendations regarding server certificates – that the certificate should have one name and that this should be set in both the CN name and subjectAltName fields – are published at https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations [1]

The above constraint arises from the following observations:

- Manual configuration of server name in Android supplicant: Android checks the server name against the Subject/CN and subjectAltName:DNS in the presented certificate - any one match is okay
- Configuration by the CAT App: Android checks Subject/CN exclusively
- Configuration by geteduroam: Android checks subjectAltName:DNS exclusively

Android 11

In addition to the above, there are currently problems specific to certain device manufacturers relating to their implementation of Android 11. These concern certain aspects of the most popular authentication methods used by organisations utilising the 802.1X standard (including all organisations participating in eduroam). Whilst workarounds are possible, the issue has resulted in unwelcome complications and difficulties for both users and organisations.

The good news is that the eduroam service development group in Europe has good connections with the developers of the Android software at the vendor concerned and the Android developers there have undertaken to rectify the bugs – expected Q2 2021.

Current problems:

- PEAP with anonymous outer identities not working for certain device manufacturers. Anything other than a few specific values (e.g. ‘anonymous@*realm*’) results in the outer identity being used as the inner identity, leading of course to auth failure. Users who set up their eduroam profiles manually do have this option to set the outer identity to be anything they choose – risking failure as the result of the supplicant using that outer identity as the inner identity. With geteduroam, you as the CAT admin control the outer identity.

  Mitigation:

  - Avoid using/disable outer IDs when using PEAP; use the CAT tool to edit your EAP Profile, in ‘General Profile properties’ ensure that the ‘Enable Anonymous Outer Identity’ tick box is **unticked.**

  - If your RADIUS system supports EAP-TTLS (not available on Microsoft NPS deployments), consider enabling this. In the CAT tool, edit your EAP Profile and in the ‘Supported EAP types’ box, move EAP-TTLS to the top of the list to make it the preferred option.

- EAP-TLS with some client certificates not working

  Mitigation - Vendor is working on resolving bug

Summary of advice

- Server certificate (for all ORPSs if you have multiple ORPS(*)): ensure that the subjectAltName:DNS field contains a certificate name (ideally one (**)) and that this matches the Subject/CN name of the certificate

- Use the CAT tool to generate eduroam profiles for your users

- Ensure that the CA Root Certificate and any CA Intermediate certificates used to issue your ORPS server certificate are uploaded to your CAT profile and that these are correct for your ORPS server certificate

- Ensure that you have specified the correct certificate name in the CN field in your CAT profile

- For Android <11 (***) your users should utilise eduroam CAT (https://cat.eduroam.org/ [2]) and the classic CAT App (https://play.google.com/store/apps/details?id=uk.ac.swansea.eduroamcat [3])

- For Android 11 your users should use the geteduroam App(https://play.google.com/store/apps/details?id=app.eduroam.geteduroam [4])

- If using PEAP, for Android 11 users, through the CAT tool disable anonymous outer identity by unticking the option box and advise users to not use anonymous outer identities unless anonymous@your [5]-realm is used

- Consider using EAP-TTLS if supported by your RADIUS deployment and configure CAT tool to select this as the preferred method in your EAP profile

(*) Multiple ORPSs: Best advice is to use one cloned certificate copied and imported for all your ORPSs. This means that only on CN name need be configured in CAT. Unique certificates can be used for each ORPS, but if so, be sure to add all cert names into your EAP profile in CAT. (CAT supports multiple CN names (+)).

(**) Multiple SubjectAltName:DNS are permissible, but you must ensure that one SubjectAltName:DNS name matches the CN name. See cert guidance at: https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations [1]

(***) Although our limited tests indicate that Android 10 works okay with geteduroam

(+) There is a known issue with ChromeOS in that when multiple CN names are configured in a CAT profile, the ChromeOS configuration file generated by the CAT system will contain SubjectMatch of only the highest level common domain (e.g. .ac.uk). This a result of the ChromeOS configuration file format (published by Google) lacking support for regular expressions. This represents a security flaw since client device CN name validation is ineffective with ChromeOS when multiple CN names are set. Mitigate this by cloning your server cert to all ORPSs and use one CN name and one SubjectAltName:DNS (that match).

Note, there are server certificate checking functions available on the CAT website (Realm Reachability Test) and the new [Certificate Check] button on your Troubleshoot page on https://support.eduroam.uk *[6]*

Comments and feedback welcomed.

Source URL: https://community-stg.jisc.ac.uk/library/network-and-technology-service-docs/2021-04-advisory-android-11-configuration-issues

Links
[1] https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations
[2] https://cat.eduroam.org/
[3] https://play.google.com/store/apps/details?id=uk.ac.swansea.eduroamcat
[4] https://play.google.com/store/apps/details?id=app.eduroam.geteduroam
[5] mailto:anonymous@your
[6] https://support.eduroam.uk