Roaming with third parties based on Passpoint

(this is a work in progress)

Service Provider settings

Third-party SPs

Third parties should use the eduroam Roaming Consortium Organisation Identifier (RCOI)

```
001bc50460 [configured in end-user device to be displayed as: "eduroam® Hitchhiker" (name provisional)]
```

to indicate that their Passpoint network is willing to accept eduroam guests. For the actual request routing, there are three possible ways:

a) negotiate a RADIUS AAA server address and shared secret with an eduroam NRO, to be used as uplink for authentications.Then, either

> a1) send all realms not belonging to another roaming partner to the eduroam servers (a "default" routing to eduroam). This is only possible if all other roaming partners at the hotspot are identifiable and can be enumerated.
>
> a2) use equipment that supports Passpoint R3 to allow identifying and forwarding of the thousands of realms in eduroam towards that one server (by leveraging the then-present RADIUS attribute "HS2.0 roaming consortium" [Vendor-Specific, Vendor 40808, Attribute 6] in the authentication request).

b) get a roaming certificate for usage with RADIUS/TLS and Dynamic Server Discovery (e.g. from OpenRoaming or from eduroam directly) and look up DNS NAPTR records for the realm in question; the NAPTR labels being "x-eduroam:radius.tls" (if you have a RADIUS/TLS server certificate from eduroam) or "aaa+auth:radius.tls" (if you have any other server certificate, e.g. an OpenRoaming one). Connections should be attempted to all servers resulting from the respective DNS responses.

eduroam SPs

There are currently no plans to move away from using the **SSID** "eduroam" as the single user-facing identifier for hotspots operated directly by an eduroam participating organisation. If this ever changes, the Roaming Consortium Organisation Identifier

```
001bc5046f [configured in end-user device to be displayed as: "eduroam®"]
```

is reserved for that purpose. It is configured in supplicants but not expected to be emitted by any SP at this point.

However, eduroam SPs which deploy a separate onboarding SSID can benefit from the Online Sign-Up capabilities in Passpoint R2 and above. They should configure their eduroam SSID to emit the OSU (Online Sign-Up) portions of Passpoint and configure the OSU server URL as defined below as the target server for Online Sign-Up. Their onboarding SSID must then allow access for end-users to that URL and to eduroam CAT.

Identity Provider settings

eduroam Identity Providers interested in letting their users authenticate in a third-party roaming scenario may need to implement some elements of the eduroam Service Definition which are typically only optional.

OpenRoaming

In particular, for participation in OpenRoaming, the following is REQUIRED:

- generating Chargeable-User-Identity attributes in authentication responses
- populating a DNS NAPTR record for their realm pointing to the eduroam OpenRoaming Interchange Proxy:

```
realm.name. 43200 IN NAPTR 100 10 "s" "aaa+auth:radius.tls" "" _radsec._tcp.TBD.eduroam.org.
```

Infrastructure

OpenRoaming

eduroam plans to operate one central interchange point with OpenRoaming. Third-party SPs find it automatically by looking up NAPTR records in DNS for aaa+auth for the respective realm.

Passpoint Release 2: Online Sign-Up

eduroam plans to operate an OSU server which directs unprovisioned end-users to the eduroam CAT toolset. The provisional URL for this server is

```
https://cat-osu.eduroam.org/soap/?idp=X
```

End-User Device settings

Starting with version 2.0.3, the eduroam onboarding toolset (eduroam CAT and eduroam Managed IdP) automatically inject network definitions based on the eduroam Roaming Consortium Organisation identifiers (RCOI) on all platforms where this is possible. The platforms and their respective caveats are listed below.

In general, the Passpoint configuration configures two eduroam RCOIs:

```
001bc50460 [Display Name "eduroam® Hitchhiker" (name provisional)]
001bc5046f [Display Name "eduroam®"]
```

The latter one is reserved for a distance-future use, in case eduroam would go fully Passpoint and give up on SSID-based configurations throughout all SPs world-wide. The RCOI would then signify eduroam self-operated hotspots with this "home" display name.

Windows before 10

These platforms are not configured for Passpoint.

Windows 10

Both for eduroam CAT and eduroam Managed IdP, the SSID-based and the Passpoint profile are installed in sequence. The SSID based configuration always succeeds. Installation of the Passpoint profile may fail if the chipset and driver on the machine does not support Passpoint. Such failures are silently ignored; no user inconvenience.

As of October 2019, there are field reports that some 10-20% of devices which do claim Passpoint support and which will be configured with Passpoint do not actually work post-config. These failures are occuring for all Passpoint configurations, i.e. are independent of eduroam; but they also do not cause any harm to the end user - the authentication and connection to Passpoint networks is simply not possible then. Up-to-date drivers are reported to help in such situations.

Apple (Mac OS X, macOS, iOS, iPadOS)

For eduroam Managed IdP, Passpoint-based profiles are always installed alongside the SSID-based ones. This is expected to work throughout the product palette of Apple, and with no additional user interaction.

For eduroam CAT, Passpoint configuration is only installed if the IdP's chosen EAP type is "EAP-TLS" as this EAP type does not trigger multiple prompts for usernames and passwords. For all password-based EAP methods, only the SSID-based configuration is pushed to the device. Apple personnel is aware of the annoyance of multiple username/password prompts and installation of Passpoint configurations alongside SSID-based ones will be enabled as soon as the situation ameliorates.

Android

The eduroam CAT app needs an update to support configuring Passpoint networks.

(The built-in method of Passpoint R1 provisioning as described in AOSP: Wi-Fi Passpoint R1) is not generally usable as the installation of new, dedicated Wi-Fi root CAs is prohibited by Android API.)

Linux

TBD.

ChromeOS

TBD.

Policy

GeGC to decide on terms and conditions for letting random SPs serve eduroam users.

Back to top