InCommon eduroam SP Testing

Date: 8-March-2022 Version: 0.91

Executive Summary

This paper presents a proposed solution to InCommon's eduroam subscribers' requirement for Service Provider (SP) testing. The solution builds on GÉANT's eduroam CAT and Managed IdP tools, and integrates with the InCommon Federation Manager. This allows InCommon to benefit from existing and proven technologies, which help to control cost and risk, and reduce time-to-market.

1. Problem statement

Eduroam enables roaming users associated with a subscribing Identity Provider (IdP) organization to connect to a Wi-Fi network operated by a subscribing SP organization.

An SP that onboards onto eduroam must deploy and configure various technologies to offer a compliant Wi-Fi network. This can be a complex process, and so it is not uncommon for SPs to face challenges testing their configuration.

This is exacerbated by the need to verify that the SP can authenticate credentials issued by another IdP. Therefore, this problem is also shared by SPs that are also IdPs. However, at present SPs cannot easily obtain credentials to test their configuration.

It is possible for an SP to approach an existing IdP and request assistance. However, this has some drawbacks:

- the SP must identify, approach and request test credentials from a cooperative IdP
- the IdP must take responsibility for the use of these credentials, and
- the IdP may also need to expend resources to help the SP configure a test device and troubleshoot any authentication issues.

The difficulty to obtaining and using test credentials can have the following consequences:

- some SPs are misconfigured, diminishing end users' experience of the service
- some SPs may become dissatisfied with the service (e.g., if they receive complaints from visitors) and unsubscribe, and
- some IdPs will bear a cost in helping to troubleshoot SPs' configurations.

This issue is likely to be particularly pronounced within new eduroam user communities because they are more likely to lack contacts with other IdPs.

2. Requirements

Table 1 below enumerates the requirements of the solution.

ID	Name	Description	Mandatory
1	End-to-end authentication	The solution must facilitate an end-to-end authentication identical to the standard eduroam connection workflow.	Y
2	Easy to use	The solution must be usable by a typical wireless network administrator. It should not require any specialist knowledge of eduroam or its technologies. It should not have any unusual dependencies or requirements.	Y
3	Support common devices	The solution must allow testing from common devices. This will make it easier for SP administrators to use the solution.	Y
4	Integration with Federation Manager	Credentials must be requested and delivered by SP administrator using Federated Manager. This will allow InCommon to offer a “single pane of glass” experience.	Y
5	Self-service	The solution must be fully self-service. This will provide a simple experience for SP administrators and avoid support costs for InCommon or other IdPs.	Y
5	Time expiry on credentials	The credentials must expire after a configurable period of time. This will reduce the potential for misuse of test credentials.	Y
6	Location-based authorisation	The credentials must only be valid at a configurable service location. This will reduce the potential for misuse of test credentials.	Y
7	InCommon-managed credentials	The credentials must be managed by InCommon. This will reduce the potential for misuse of test credentials and avoid requiring IdPs to take responsibility for credentials issued to SPs.	Y
8	Integration with eduroam logging	The eduroam logging system must expose logs of test authentications with SPs. This will make it easier for SP administrators and InCommon to troubleshoot problems.	N
9	Browser-based diagnostics	The solution must perform diagnostics related to the service location where the testing is performed. This could make it easier to onboard SPs (e.g., by automatically provisioning service location data into FM) and provide InCommon with a better understanding of service provision.	N

Table 1

3. Proposed Solution

This document proposes a solution based on InCommon's Federation Manager, and GÉANT's eduroam CAT and Managed IdP tools.

3.1 eduroam Configuration Assistance Tool

The Configuration Assistance Tool ("CAT") is both a tool developed by GÉANT. It builds customized installers for a range of platforms and enhances the security for the end user by ensuring robust platform configurations. It is used widely by organizations across the EU, US and other regions. Today, there is only a single instance of the CAT tool, which is operated by GÉANT.

We propose using the CAT as the delivery platform for test credentials and the browser-based diagnostic tool to SPs. The CAT will not be exposed to SP administrators.

3.2 eduroam Managed IdP

The Managed IdP ("MIdP") is an optional feature of the CAT tool, also developed by GÉANT. It enables eligible institutions to outsource their eduroam IdP functions to the eduroam Operations Team. IdP administrators use the service instead of local authentication infrastructure and identity management. Today, there is only a single instance of the MIdP tool, which is operated by GÉANT.

We propose using the MIdP to manage the SP credentials. These credentials will be short-lived x.509 certificates. The MIdP provides the tools needed to administer the Certification Authority responsible for these certificates. The MIdP will not be exposed to SP administrators; instead, Federation Manager will act as a frontend.

3.3 Federation Manager

The Federation Manager ("FM") enables authorised users to manage their organization's eduroam service technical configuration. We propose using FM as the interface to installers provided by CAT and MIdP. FM will need to be extended to:

- offer SPs the option to download an installer containing their test credentials, and
- the ability to use the MIdP's APIs to manage SP credentials (create, revoke, etc)

Optionally, FM could also be extended to:

- integrate with the browser-based diagnostics tool described next, and
- integrate with the eduroam logging system to expose logs of test authentications to SP administrators.

3.4 Browser-based diagnostics

This functionality is not directly related to SP testing, and so implementation could be deferred to a later point.

The CAT offers the option to open a URL using a web browser after a successful authentication. This could be used to deliver a browser-based diagnostics tool. This could acquire a rich variety of information about the SP's service location, such as:

- the service location's geographic location
- whether IPv4 and/or IPv6 are available, and
- the effective upstream and downstream network capacity.

These diagnostics could be helpful for both the SP and InCommon; for example, to automatically populate a service location's geographical location within FM.

3.5 Solution match against requirements

Table 2 below describes how the solution addresses the requirements set out in Table 1.

ID	Requirement	How is the requirement met	Feature
1	End-to-end authentication	The solution uses the test device's native supplicant, configured by CAT, to perform an end-to-end authentication across the eduroam infrastructure against an IdP managed by InCommon	Test credentials can be used to perform an end-to-end test
2	Easy to use	From the perspective of the SP administrator, the solution uses FM and installers provided by CAT. These are proven and familiar products that are easy to use. SP administrators will not use MIdP or CAT directly. Instead, FM will orchestrate these tools to allow seamless provision of a CAT installer that includes the test credentials.	Test credentials are provided to the SP within installers for common devices
3	Support common devices	The solution uses CAT, which supports all common devices.	Test credentials are provided to the SP within installers for common devices
4	Integration with Federation Manager	Credentials are requested and delivered by SP administrator using Federated Manager.	Test credentials are provisioned through FM
5	Self-service	The solution is fully self-service through FM.	Test credentials are provisioned through FM
5	Time expiry on credentials	The credentials expire after a configurable period of time. This will be controlled by using short-lived certificates as the test credentials.	Test credentials are short-lived X.509 certificates
6	Location-based authorisation	The credentials are only be valid at a configurable location. This will be controlled through policy at the MIdP.	Test credentials are scoped to an SP service location
7	InCommon-managed credentials	The test certificate credentials will be issued and managed by a certification authority, which is provided as part of MIdP. MIdP will be operated by InCommon.	Test credentials are provisioned through FM
8	Integration with eduroam logging	The eduroam logging system could expose logs of test authentications to SPs by correlating the credentials to the relevant SP.	Test credentials can be correlated centrally with TLRS logs
9	Browser-based diagnostics	The solution could perform browser-based diagnostics related to the service location where the testing is performed using a URL supplied within the CAT installer.	The installer can invoke browser-based diagnostics

Table 2

4. Value proposition

Table 3 below summarizes the value proposition of the proposed solution.

Features	Advantages	Benefits
Test credentials can be used to perform an end-to-end test	SP can verify that their eduroam service is working	SP can confidently offer an eduroam service to end users
Test credentials are short-lived X.509 certificates	Credentials are valid for a short period of time, reducing the potential for misuse	Trust in eduroam is maintained
Test credentials are scoped to an SP service location	Credentials can only be used at authorized service locations, reducing the potential for misuse	Trust in eduroam is maintained
Test credentials are provided to the SP within installers for common devices	SPs can easily configure a device locally to test with	Testing can be completed quickly and easily
Test credentials are provisioned through FM	SPs can easily obtain test credentials from InCommon, an expected and trusted provider, without involving any other parties	Testing can be completed quickly and easily Trust in eduroam is maintained IdPs do not bear the cost of helping InCommon to onboard SPs
	InCommon can control the issuance of test credentials	Trust in eduroam is maintained
	InCommon can easily revoke and control the appropriate use of the credentials	Trust in eduroam is maintained
Test credentials can be correlated centrally with TLRS logs	It is easier for SPs and the InCommon helpdesk to troubleshoot issues	Testing can be completed quickly and easily IdPs do not bear the cost of helping InCommon to onboard SPs
The installer can invoke browser-based diagnostics	The SP and InCommon can easily acquire Information about characteristics of the SP's service location	SPs and InCommon can use diagnostic information to improve their services

Table 3

An SP testing capability will:

- improve the end user and SP experience of the service by making it quicker and easier to complete SP testing
- enhance trust in eduroam by reducing the need to distribute of credentials, and
- reduce costs for IdPs in their helping SPs to test their deployment.

In addition, the SP testing capability offers the potential for providing other enhancements that could be valued by subscribers and/or helpful for InCommon. Examples of candidate enhancement are browser-based diagnostics and integration with eduroam logging.

5. Architecture

The high-level architecture for the proposed solution is shown in Figure 1.

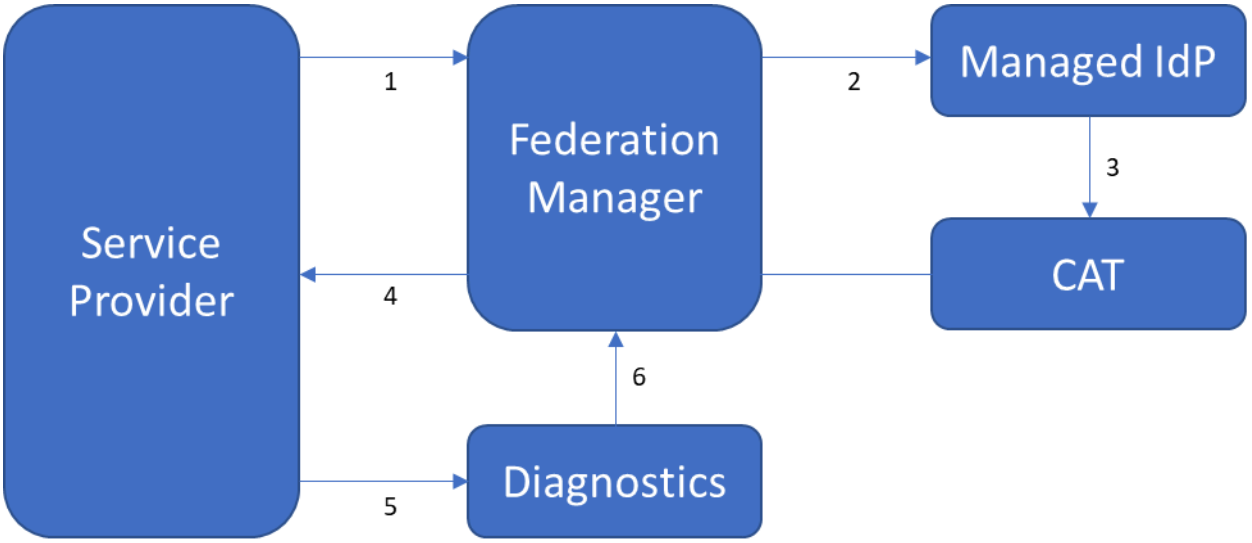

Figure 1

The general workflow proceeds as follows.

1. The SP administrator requests a test account from FM.
2. FM uses MIdP's API to create an account and credential for the SP administrator.
3. MIdP creates installers which are signed by CAT.
4. The installers are made available for download via FM to the SP administrator. The SP administrator can execute the installer, and attempt to perform a test authentication. The certificate is only authorized for use at the SP's own service locations.
5. If authentication is successful, the browser-based diagnostics is invoked.
6. The diagnostics tools gathers information about the service location and provides the data to FM.

6. Approach

We propose a project having the following workstreams and key deliverables.

1. Architecture
    a. **Liaison with GÉANT**. The GÉANT CAT and MIdP development teams understand their tools best. We will work with these teams to understand the software, benefit from their knowledge, and align development roadmaps and practices.
    b. **Discovery and design**. Although the solution builds on three existing products, we will still need to develop a detailed architecture for the solution owing to the integration and orchestration requirements.
2. Infrastructure
    a. **Infrastructure development**. We will need to create new infrastructure to instantiate the MIdP and CAT instances operated by InCommon.
    b. **Prepare for operations**. Various aspects of the solution will need to be configured, documented, and aligned with other infrastructure components to ensure that the solution can be delivered effectively.
3. Software
    a. **FM extensions**. FM will need to integrate with InCommon's MIdP and CAT instances.
    b. **MIdP extensions**. MIdP will need support for location-based authorisation.
    c. **Browser-based diagnostics (optional)**. We could develop a browser-based diagnostics tool. This would also require additional extensions to FM.
    d. **Integration with eduroam logging (optional)**. We could extend the eduroam logging system to expose test authentication logs to SP administrators.
4. Piloting
    a. **Test the solution**. We will test the performance of the solution with some SPs against metrics derived from the solution requirements.
    b. **Assess performance**. We will decide if the solution is ready for service based on its performance during testing and other relevant factors.

6.1 SWOT analysis

Table 4 below gives a preliminary SWOT analysis.

Strengths	**Weaknesses**
● Ability to "spin up" and "fail fast" with minimal investment by leveraging GÉANT's existing tools ● Timely delivery by using GÉANT's existing tools ● Low operational risk	● MIdP is relatively new and less proven than CAT ● Limited experience of either tools resulting in some risk ● Some costs will be incurred in extending FM and MIdP
Opportunities	**Threats**
● Potential for collaboration with GÉANT ● Use of FM as a frontend allows other tools to be more easily used/substituted in the future	● None identified

Table 4