



eduroam Managed IdP

Product Presentation

Stefan Winter

GeGC Technical Expert, Task Leader eduroam Development @GEANT

R&D Engineer, RESTENA Foundation, Luxembourg

Last updated: 13 June 2017

eduroam Managed IdP



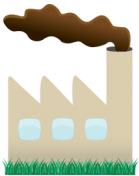
institutional eduroam IdP infrastructure



using the best technology available



run by experts from eduroam Operations Team



in professionally managed central infrastructure



controlled by you from a web browser

- Target Groups:
 - Institution administrators who do not have the skills or capacity to run their own RADIUS IdP infrastructure
 - End-users in such institutions who want to benefit from eduroam despite the institution's incapacity
 - NROs wishing to add more value to their national eduroam offering; and/or who wish to widen their institution-level coverage
- Product offers:
 - Technical outsourcing of all aspects of user management
 - Create, change users
 - Provision, revoke, expire credentials for users
 - Provide status information about user credentials
 - Provide interface to identify user in case of abuse
- Product does NOT offer:
 - Liability for end user accounts created with this system

- eduroam Managed IdP is using work flows and technological foundation of eduroam CAT
- Eligibility and governance follow exactly the eduroam CAT way
 - Anchor point: NRO administrators (invited to Operations Support Services via “realm.xml” denomination)
 - All NROs world-wide can enable or disable the functionality for their NRO (see screenshot “NRO”)
 - NROs invite institutions to eduroam Managed IdP via the established process
- Institutions create exactly one Managed IdP profile where they can manage a user base, but do not have to care about EAP technical details (see screenshot “IdP”)

eduroam Configuration Assistant Tool View this page in

English(GB) ▾

Administrator Interface - Federation Management


eduroam managed IdP Pilot Phase

Federation Overview

Your Personal Information

E-Mail Address **stefan.winter@restena.lu**
Real Name **Stefan Winter**
Federation Administrator **LU**
Unique Identifier [click to display](#)

Federation Properties: Luxembourg

Country **Luxembourg**
Federation Logo 
Federation Operator Name default/other languages **RESTENA Foundation**
Federation Operator Name (unsupported language) **Fondation RESTENA**
Enable Managed IdP **on**

Edit

Screenshot: IdP



Current institution users

The assigned realm 13-12.lu.test.hosted.eduroam.org
The total number of active users which are allowed for this profile 200
The current number of configured active users 1
The current number of configured inactive users 0

Manage institution users

User	Token/Certificate details	User Expiry/Certificate Expiry	Actions	
swinter	Device:Apple macOS Sierra Serial Number:3a6275da7 CN:fctVncWR4yRzX7bE88NQLfbbwGtwdAr@... Expiry:2020-12-16 Revoke	Device:Apple macOS Sierra Serial Number:54accb3ee CN:wetTv7O9iAJGDN3xYmkTVDDUu8Ahxt@... Expiry:2020-12-16 Revoke	Device:Apple macOS Sierra Serial Number:14f419cba3 CN:JBVncoHYzQh9NgmGgyoN9ofxFm6TIiv@... Expiry:2020-12-16 Revoke	
	Device:Apple macOS Sierra Serial Number:a2b6bf54c CN:XMzzEADFJJuFeNQwyn9NrpC6y6AHT2C@... Expiry:2020-12-16 REVOKED			
	<input type="text" value="https://cat-pilot.eduroam.org/accountstatus/accountstatus.php?token=567ff675e8217a64e79720584116d81dbcd227c857611"/> Copy to Clipboard Compose mail...		2020-12-17 Update	Deactivate User New Credential
			2017-06-20	Revoke

You need to acknowledge that the created accounts are still valid within the next 287 days. If all accounts shown as active above are indeed still valid, please check the box below and push "Save". If any of the accounts are stale, please deactivate them by pushing the corresponding button before doing this.

I have verified that all configured users are still eligible for eduroam

Save

Add new user

Import users from CSV file

Please enter a username of your choice and user expiry date to create a new user:

▼

Add new user

Screenshot: end-user download interface



eduroam managed IdP Pilot Phase

Welcome to eduroam CAT

eduroam Configuration Assistant Tool

View this page in [English\(GB\)](#)



[Start page](#)

Your personal eduroam account status page

Your invitation token is valid. You can now create an installation program with personalised eduroam login information.

The installation program is **strictly personal**, to be used **only on the device** you are currently using (Linux), and it is **not permitted to share** this information with anyone. When the system detects abuse such as sharing login data with others, all access rights for you will be revoked and you may be sanctioned by your local eduroam administrator.

During the installation process, you will be asked for the following import password. This only happens once during the installation. You do not have to write down this password.

Import Password: rd6UPV

[Click here to download your eduroam installer!](#)



Showcase for Managed
IdP Demonstration



eduroam National
Roaming Operator in
Luxembourg


- Individual accounts are created by institution administrator
 - Analogous to the creation of a user in a local IDM system
 - Merely the location of the user database is not local at the institution, but inside the Managed IdP infrastructure
 - The responsibility for these accounts, i.e. they
 - pertain to actual humans
 - are currently members of the institution in question
 - are considered eligible for the eduroam service
 - can be contacted and reprimanded when abusing the servicerest with the administrator!
- eduroam Managed IdP platform provides technical means to make the link between an access credential and a user in the system
 - Institution administrators can find out which user account name is behind a (pseudonymous) access credential.
 - Anyone can find out to which institution an access credential belongs.

- **Strive towards: no data which can be considered personally identifiable should be stored at all.**
- Admin (himself known only by his ePTID or equivalent)
 - Creates accounts for end-users
 - These are simply strings
 - They do not need to be (and we don't ask for) strings that can be linked to actual humans.
 - Ex.: "localuser123" is perfectly fine as a username, and not PII
 - Only the admin himself, locally, has to be able to make a link between the usernames we see and the actual human behind it
- Credentials
 - Do not even carry that username as a property. The EAP-TLS username in the client certificates is a random hash; that's the only thing being seen during authentication.
 - Only the Managed IdP database can make a link between the hash and the username chosen in the interface (and that is not a link to the human, see above)
- Authentication
 - IdP only sees the certificates (hash...) and a MAC address.
 - A MAC address is not usually considered personally identifiable data.

- System uses EAP type EAP-TLS (client certificates) for end-user credentials
- Usernames in the certificates do not reveal usernames as configured by admin
- Common root CA for all client certificates (run by eduroam Operations Team, OT)
 - Intermediate CAs per-NRO foreseen
 - Initial deployment with one central Intermediate CA for world-wide account issuance (run by OT)
 - That one CA is going to operate as an online CA in controlled premises
 - Every NRO can transition from using the central Intermediate to its own per-NRO one at any time (“nameConstraints”) (-> NRO request via the usual channels)
 - this introduces technical complexity for the NRO (!)
 - needs to run its own copy of the issuing parts of eduroam-as-a-service
 - needs to operate an online CA incl. OCSP responders
- All CAs maintain OCSP responders
 - Administrator user interfaces allows revocation of credentials
 - Revocation status is propagated immediately and checked during authentication

Screenshot: Installed on a Mac OS Sierra

JBVncoHYzQh9NmgGgyoN9ofxFm6Tliv@13-12.lu.test.hosted.eduroam.org

 **JBVncoHYzQh9NmgGgyoN9ofxFm6Tliv@13-12.lu.test.hosted.eduroam.org**
Ausgestellt von: eduroam Managed IdP Client Auth Issuing CA - PILOT
Ablaufdatum: Mittwoch, 16. Dezember 2020 um 09:50:19 Mitteleuropäische Normalzeit
⚠ Dieses Zertifikat wurde von einem nicht vertrauenswürdigen Aussteller signiert.

▶ **Vertrauen**
▼ **Details**

Name des Inhabers
Firma eduroam
Organisationseinheit LU
Allgemeiner Name JBVncoHYzQh9NmgGgyoN9ofxFm6Tliv@13-12.lu.test.hosted.eduroam.org
E-Mail-Adresse JBVncoHYzQh9NmgGgyoN9ofxFm6Tliv@13-12.lu.test.hosted.eduroam.org

Name des Ausstellers
Firma eduroam
Organisationseinheit eduroam-as-a-Service
Allgemeiner Name eduroam Managed IdP Client Auth Issuing CA - PILOT

Seriennummer 89994677155
Version 3
Signatur-Algorithmus SHA-256 mit RSA-Verschlüsselung (1.2.840.113549.1.1.1)
Parameter Ohne


Erst gültig ab Mittwoch, 31. Mai 2017 um 10:50:19 Mitteleuropäische Sommerzeit
Nur gültig bis Mittwoch, 16. Dezember 2020 um 09:50:19 Mitteleuropäische Normalzeit

Öffentlicher Schlüssel
Algorithmus RSA-Verschlüsselung (1.2.840.113549.1.1.1)
Parameter Ohne

Öffentlicher Schlüssel 256 Byte : AD 5D 89 77 92 09 0F 6A ...
Exponent 65537
Schlüssellänge 2048 Bit
Schlüsselverwendung Verschlüsseln, Überprüfen, Einpacken, Ableiten

Signatur 512 Byte : 5B F1 F6 A3 47 49 C9 6E ...

Profile

Benutzerprofile
 **eduroam**
4 Einstellungen

eduroam
Showcase for Managed IdP Demonstration **Überprüft**

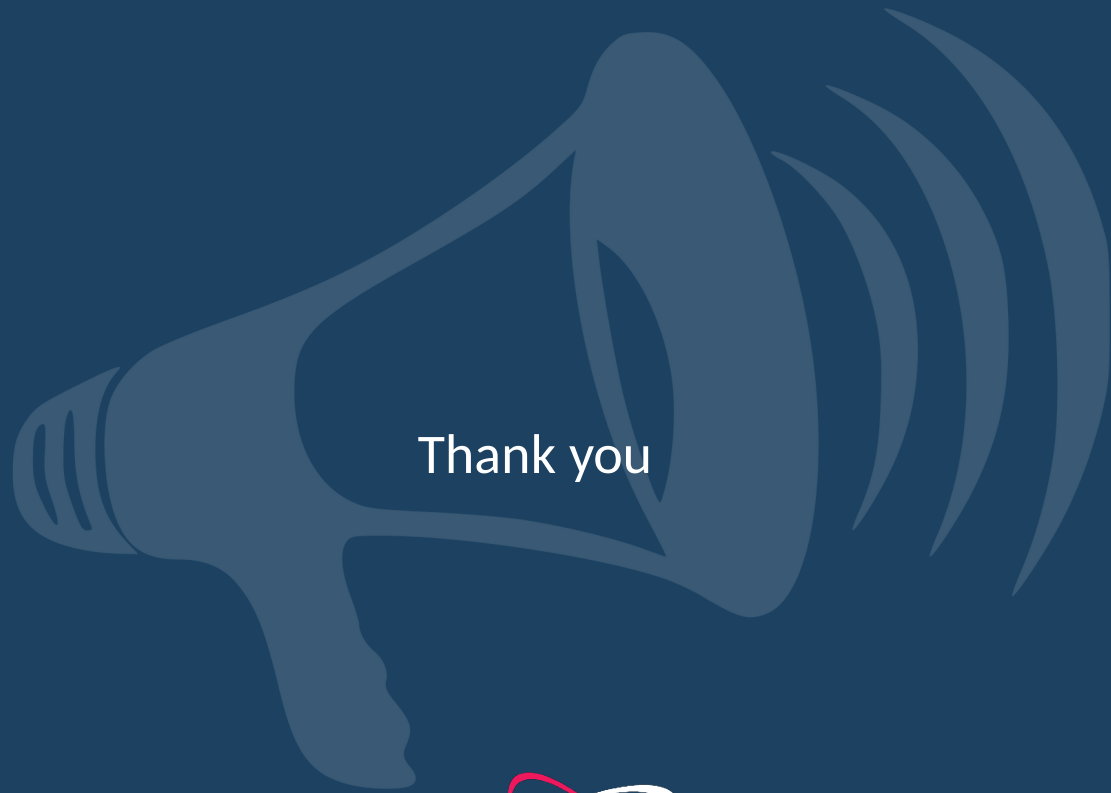
Beschreibung Managed IdP configuration for IdP 'Unnamed Institution' - provided by eduroam
Signiert GÉANT Association
Installiert 31.05.2017, 13:20

Einstellungen **Zertifikat**
eduroam-as-a-service LU Server CA Root
WLAN-Netzwerk
eduroam
Zertifikat
(2)
Passpoint-Netzwerk
13-12.lu.test.hosted.eduroam.org

- Eduroam Managed IdP comprises a RADIUS IdP server
 - Realm: ...@...TLD.hosted.eduroam.org, reachable via RADIUS/TLS NAPTRs exclusively
- Redundancy in two dimensions
 - Can be load-balanced and replicated (but remaining one logical entity)
 - Can be partitioned in per-NRO fashion (EAP-TLS termination point per country)
- To facilitate partitioning, initial deployment starts with server-side CAs and server certificates per-NRO (ca. 200 NRO personalities in one server)
- As soon as NRO wishes to run its own partition (-> NRO requests via usual channels),
 - issue new server certificate, run termination point both on central and NRO-based instance
 - Or transfer CA and private key to NRO, run termination point only on NRO-based instance
- OCSP Responders for the client certificate root CA and central intermediate CA are in responsibility of eduroam OT

- Implementation Progress
 - Working system is currently in pilot phase
 - Waiting for your evaluation, feedback and feature requests
 - <https://cat-pilot.eduroam.org>
- Manual: <https://wiki.geant.org/pages/viewpage.action?pageId=66650390>
 - Chapter 5 for NROs wishing to enable the service
 - Chapters 6+7 for IdPs
- Product includes level 1 helpdesk services (provided by GEANT Service Desk)
- We are considering to make this service a charged one due to its operational complexity and associated cost
 - Probably “TCS-style”
 - NROs pay for enabling this country-wide
 - There are several levels, criteria and price point TBD

stefan.winter@restena.lu



Thank you



Networks · Services · People
www.geant.org

