

Experiences in multi-federation TLR services and roaming

Karri Huhtanen, Radiator Software Oy



Radiator Software = Arch Red + OSC

Original Radiator product was developed by Australian Open System Consultants (OSC) since 1997.

Arch Red from Finland was originally a reseller integrator of Radiator since 2003.

In 2010 Arch Red was hired by OSC to do global integration and support for Radiator under OSC brand.

In 2012-2013 Arch Red negotiated and started the acquisition of OSC and successfully finished it in 2016.

During Arch Red control 2013-2016 the company group revenues have doubled while maintaining the profit level. The company group continues to grow profitably.


Arch Red - OSC has headquarters in Tampere (Finland), some R&D in Helsinki and some support and consultation in Australia.

In 2018 Arch Red and OSC joined under one name and brand: Radiator Software.




Radiator

Roaming in Finland

- 
- Was based on RADIUS roaming idea presented by Wirlab and Juha Heinänen in Seinäjoki 2002
 - Adapted idea presented at Funet Technical Days in 2002 as Funet WLAN Roaming

eduroam in Finland

- 
- Cooperation between Tampere University of Technology and CSC/FUNET led to contact with Terena Mobility and TNC2003 [1]
 - TNC2003 cooperation led Finland to eduroam among the first countries

The tale of two federations

Funet WLAN roaming

- Open to all organisations and companies
- Captive portal authentication, WPA/WPA2 handled by eduroam
- No common ESSID
- Ended in the end of May 2018. Members can join roam.fi if they want.

eduroam Finland

- Limited to higher education and research organisations
- 802.1X => WPA/WPA2 authentication
- Unified network name (ESSID)

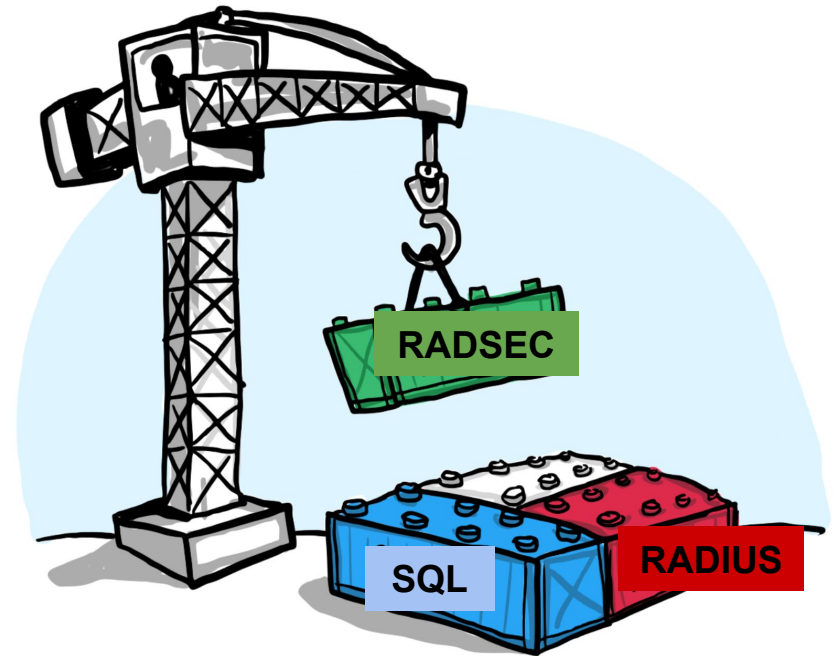
Finnish/Federation Top Level RADIUS




- First TLR was FreeRADIUS with static configuration running under Sami's desk
- Production version (2004) ran Radiator and was located in Tampere

FTLR evolution

- First, SQL database for realms and clients, FTLR2 came later with virtualisation
- Then WWW UI developed partly in Wireless Tampere community network project 2006 onwards
- Then multi-federation, RadSec, DNSRoam support presented in TNC2010 in Vilnius Lithuania [2]



Wireless Tampere (Langaton Tampere), roam.fi

- 
- From 2007 onwards, rebranding to Finland wide roam.fi 2017-2018
 - First a regional federation, which has extended (but slowly) to other regions via roaming and services
 - Designed and implemented to be “eduroam/govroam for all”
 - Roaming, IdP and captive portal as services
 - Architecture and original concept presented at TNC2008 in Bruges, Belgium [3]

Lessons learned: Technologies

- Simple, stable, fault tolerant technologies, which automate or reduce maintenance work are best choices (SQL DB, RADIUS, Linux, virtual hosts...)
- Clean design and simple solutions prevail or should prevail over more advanced ones (email address based user accounts over AD, one root service for one federation)
- Complex technologies may come for feasible when time passes, usability and provisioning technologies advance (WPA2 Enterprise, X.509 certificate based AAA, eduroam-cat, IdP as a Service ...)
 - Still waiting: RadSec, Diameter, DNSRoam, DANE, DNSSEC
- eduroam architecture and technology is future-proof

Lessons learned: Policies 1/2

- Too much freedom is bad, for example:
 - Letting members decide, if usernames work without realm, which realm to use, or if server certificate verification should be done
 - Letting members (try) to join federation with any vendor RADIUS server with any configuration member's IT people manage to do
 - Not validating member configurations, installations and conformance, accepting “dirty” traffic (e.g. MAC addresses)
 - Some configuration problems have been around for a long time [4]

Lesson learned: Policies 2/2

- Policies should not lock vendors or service providers -- all compatible solutions should be available.
- Vendors and service providers should be validated for conformance.
- Member competence and configurations should be validated -- non-competent member should be allowed to use only productised solutions for joining
- Making own policies is hard, reusing eduroam policies is easy

Lessons learned: Federation

- Be open who you accept to federation -- be strict what is required from them.
- All users should get access to federation (service) via home organisation or service provider -- especially consumers.
- Neutral federation coordinator is good, but any federation should have a product owner interested in expansion
- IdP (and SP) should be offered as a service in any federation -- good way to secure conformance with productised solution.
- Productised configurations and solutions should be preferred and developed together with vendors, service providers and competent members.

Lessons learned: Multiple Federations

- Managing multiple federations with same root service is complex -- one root service for one federation is more simple and clean.
- Unless single federation is able to accept all and be accepted by all, the need for multiple federations exists (eduroam, govroam, roam.fi ...)
- Defining roaming protocol and policies between federations would help to extend federation coverage and usability without trying to converge into one federation model. This would also help IdP providers to provide services for multiple federations.
- Because no federation really wants to define policies from scratch, eduroam policies could be open basis for any federation policy.

Thank you. Questions, Comments?

for more information

Karri . Huhtanen (at) radiatorsoftware . com

Twitter: khuhtanen

Google+: <https://plus.google.com/+KarriHuhtanen>

References

- [1] Applying Radius-based Public Access Roaming in the Finnish University Network (FUNET): <https://tnc2003.terena.org/programme/papers/p8d1.pdf>
- [2] Implementing multi-federation and peer-to-peer roaming on the eduroam federation level: <https://tnc2010.terena.org/schedule/presentations/show/62/>
- [3] Utilising eduroam architecture in building wireless community networks: https://tnc2008.terena.org/schedule/presentations/show823e.html?pres_id=66
- [4] eduroam diagnostics in NTLR, IdPs and SPs: <https://www.slideshare.net/khuhtanen/eduroam-diagnostics-in-ntlr-idps-and-sps>