

PROGRESS AND CHALLENGES IN INTRODUCING EDUROAM AND FEDERATED IDENTITY IN BANGLADESH

PREPARED AND PRESENTED BY

MOHAMMAD TAWRIT

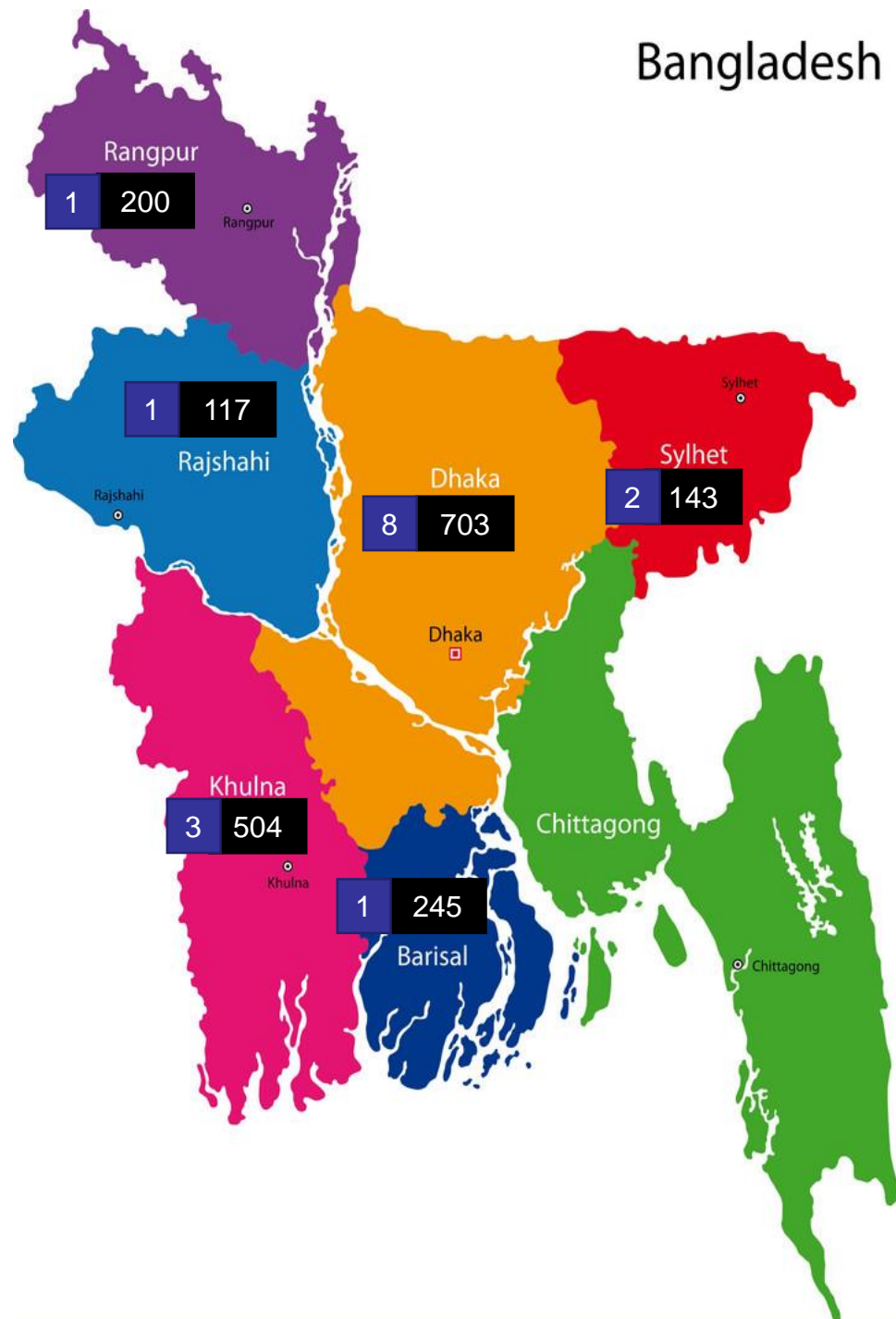
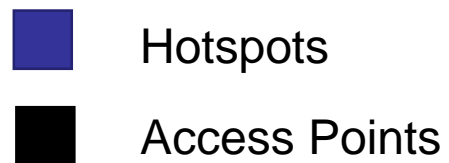
CEO, BDREN

DATE: 18 DECEMBER, 2019



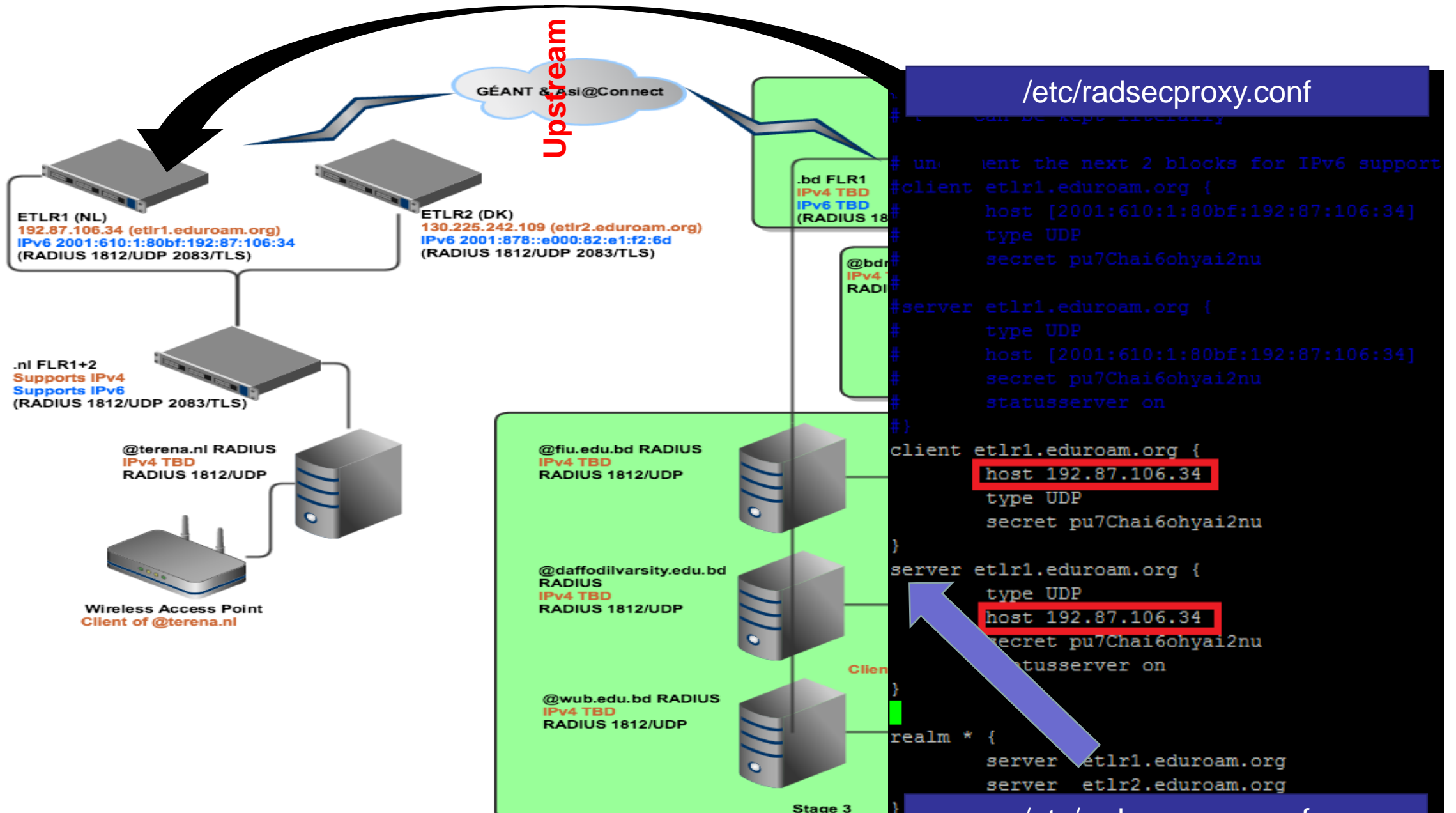
Eduroam in Bangladesh

| Hotspots | University/Institute | Date of Deployment | Number of Access Points |
|----------|----------------------|--------------------|-------------------------|
| 1 | BdREN | July, 2017 | 5 |
| 2 | SBAU | August, 2017 | 12 |
| 3 | SUST | September, 2017 | 100 |
| 4 | BUET | November, 2019 | 273 |
| 5 | IUB | November, 2018 | 80 |
| 6 | SAU | January, 2019 | 43 |
| 7 | MBSTU | April, 2019 | 119 |
| 8 | JUST | July, 2019 | 149 |
| 9 | PSTU | August, 2019 | 245 |
| 10 | PUST | September, 2019 | 117 |
| 11 | DUET | September, 2019 | 146 |
| 12 | BRUR | September, 2019 | 200 |
| 13 | KUET | November, 2019 | 329 |
| 14 | IU | November, 2019 | 26 |
| 15 | BSMRAU | December, 2019 | 60 |
| 16 | IUT | November, 2019 | 8 |
| Total | | | 1912 |



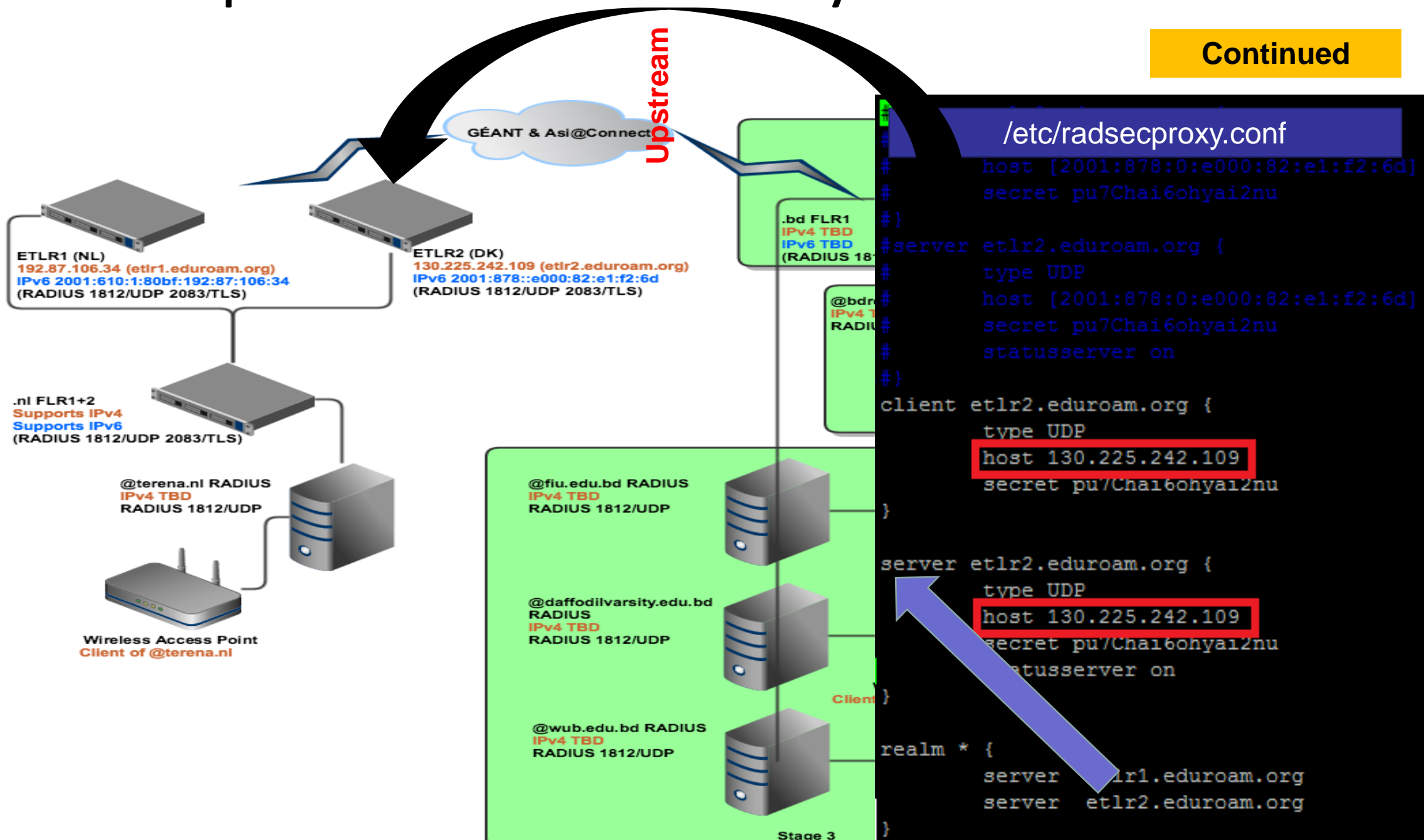
- Total Hotspots: **15**
- Total Access Points: **1904**

Upstream Connectivity - Netherland

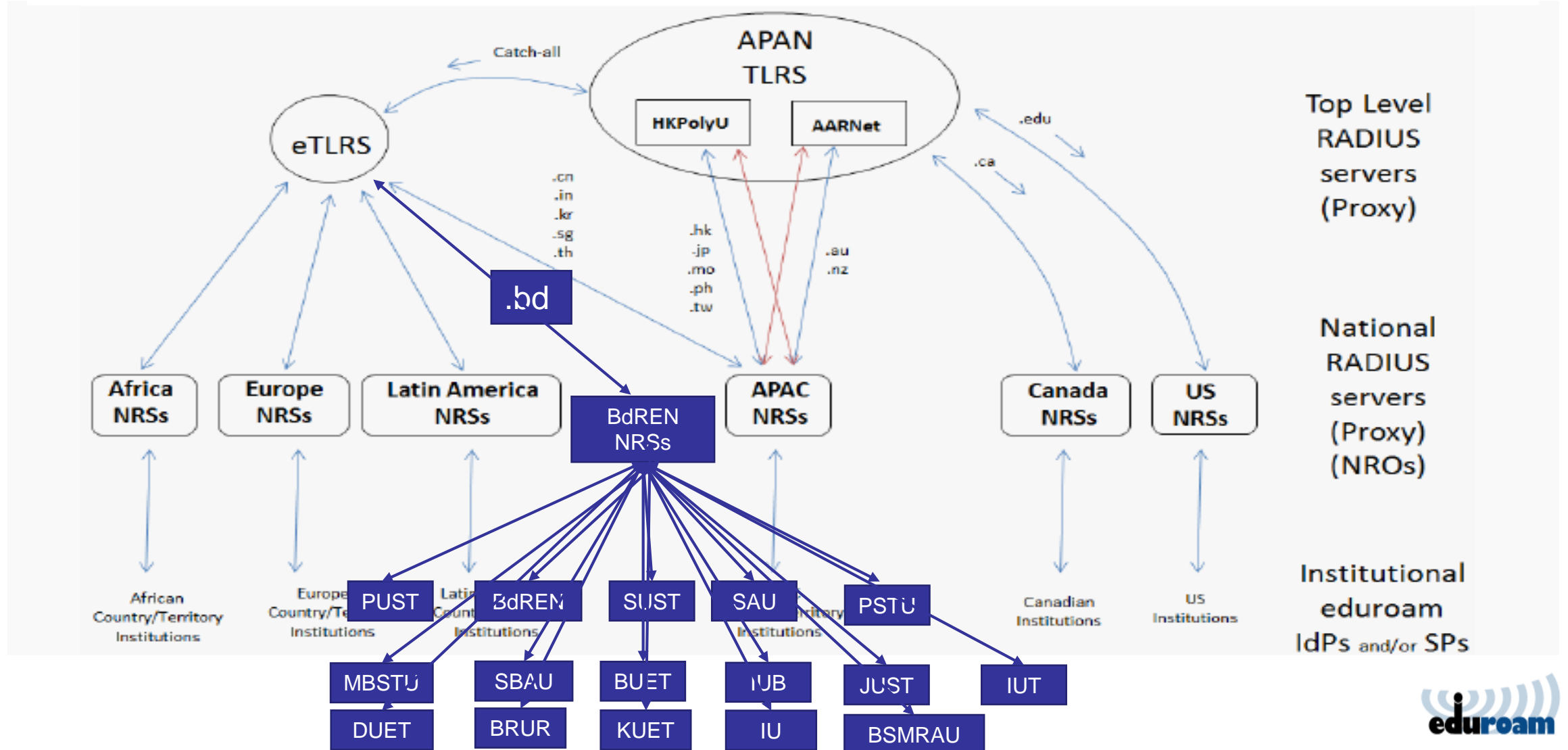


Upstream Connectivity - Denmark

Continued

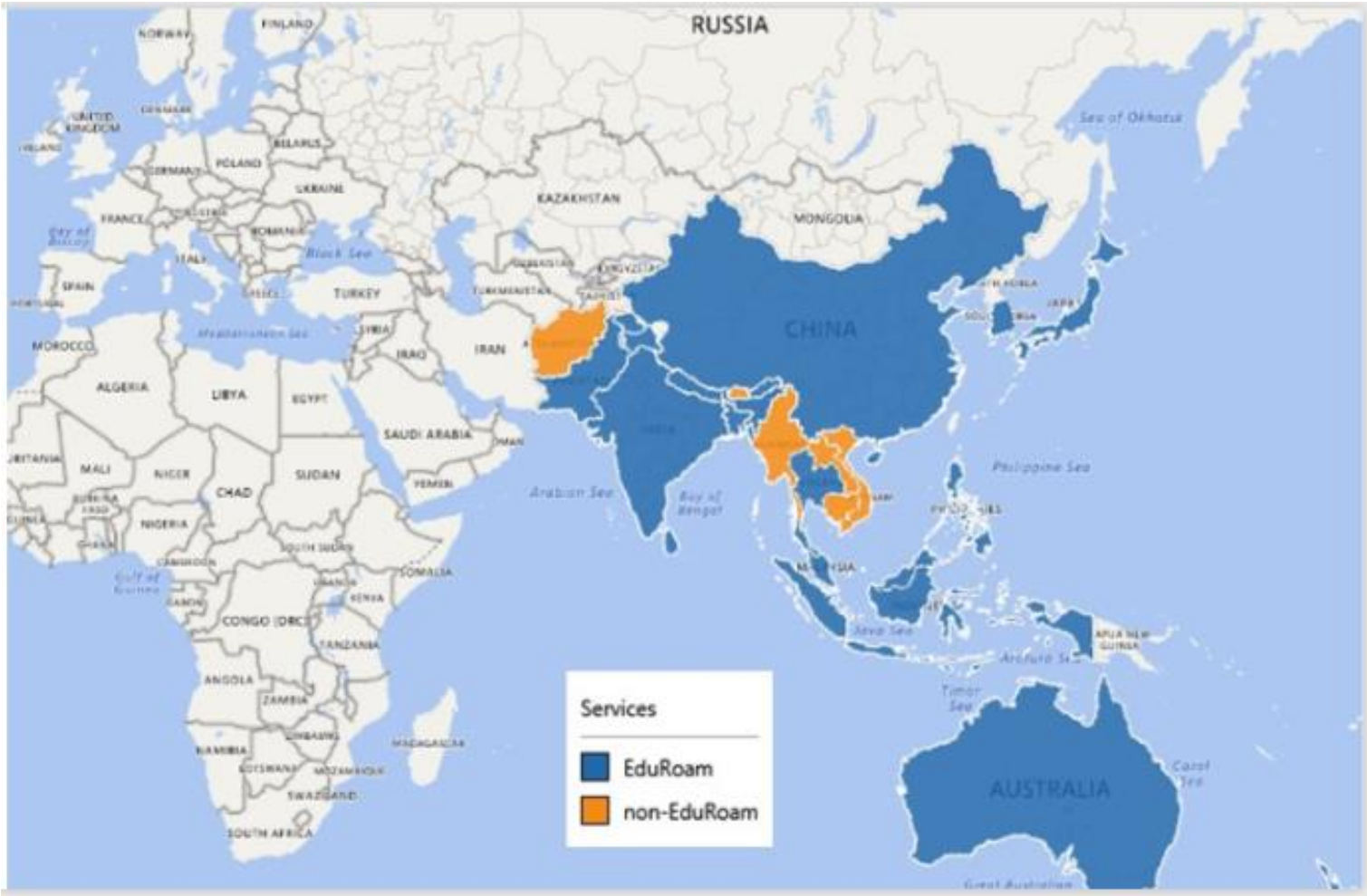


Flow of Trust



Eduroam Coverage in Asia

<https://www.eduroam.org/where/>



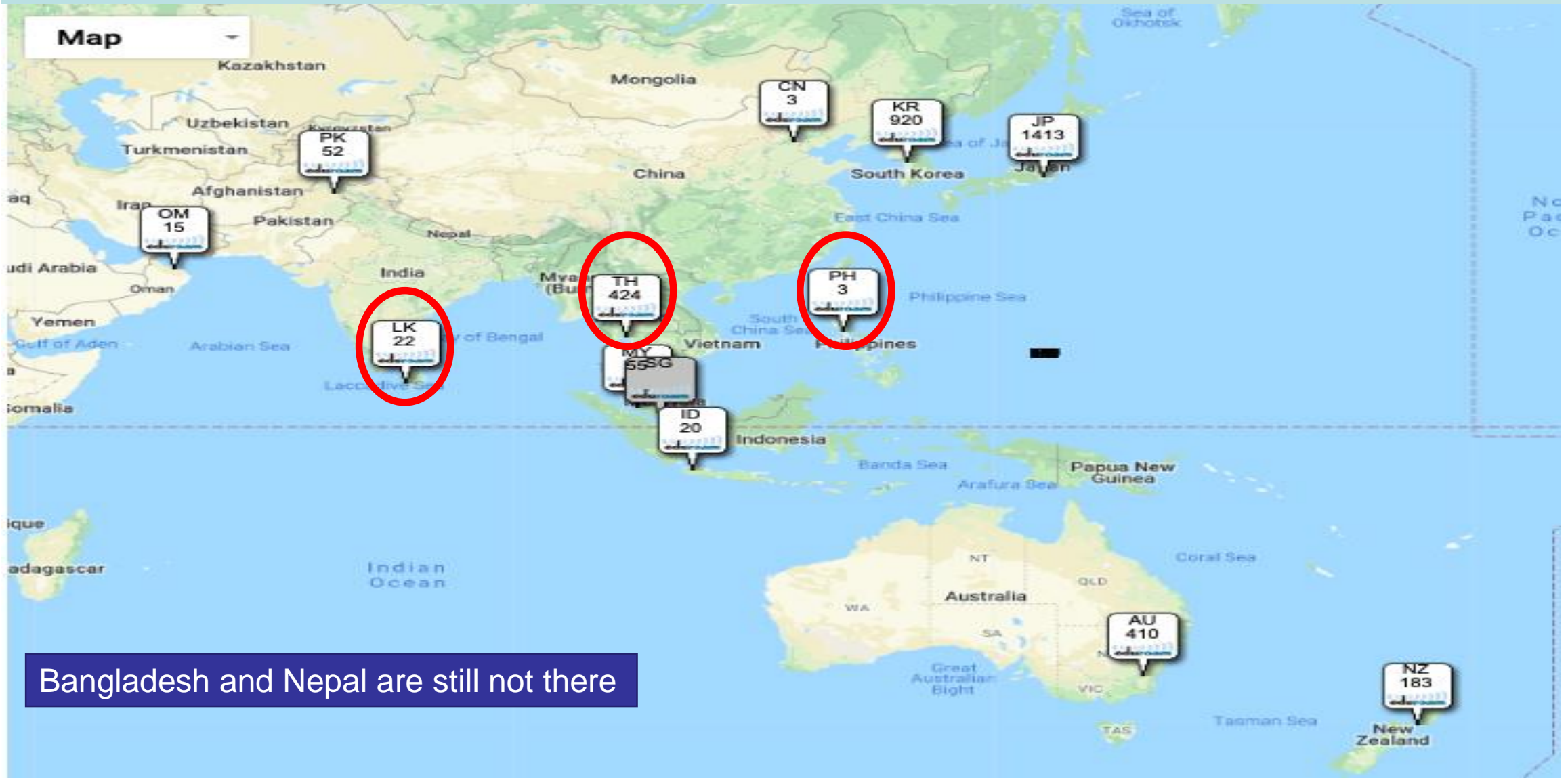
Other than very few countries like Afghanistan, Bhutan, Cambodia, Myanmar and Laos almost all other countries in Asia has established Eduroam in their country.

All Partnering countries in fDLuDCf has established eduroam service out of total 101 countries

Bhutan is included as one of the 18 countries who are under Pilot project

Partnering Country Statistics (Monitoring)

https://monitor.eduroam.org/map_service_loc.php



Bangladesh and Nepal are still not there

Concerns?



<https://www.eduroam.org/configuration-assistant-tool-cat/>
Is Eduroam secured? **Yes.....**
If and only if, the user cares enough that he wants to get connected to his own IdP

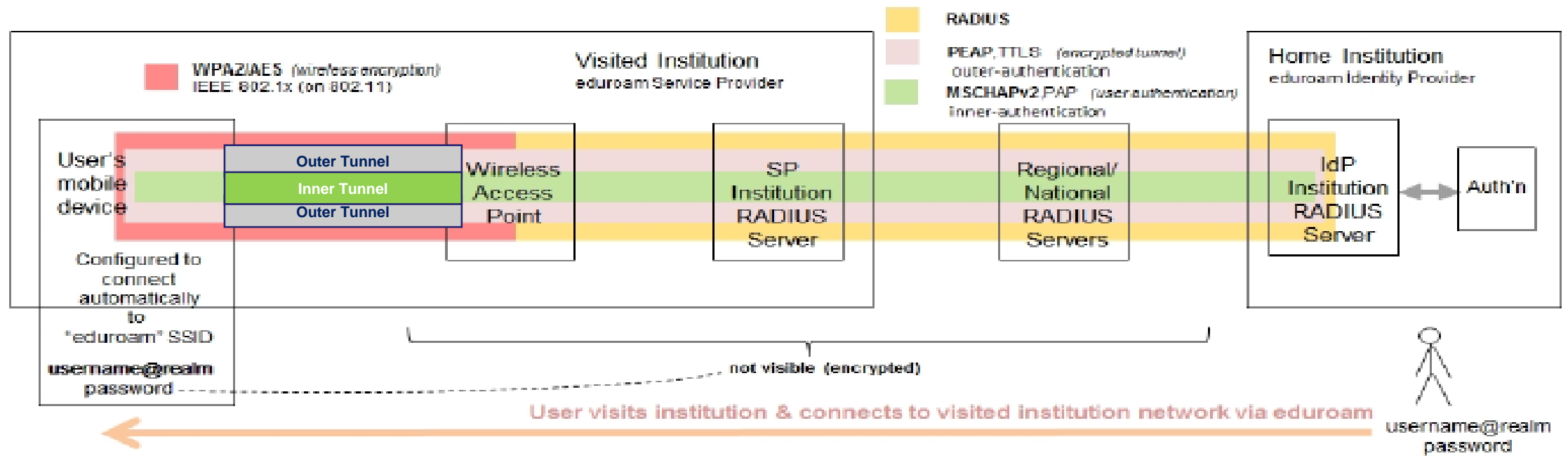
<https://www.eduroam.org/eduroam-security/>

Is eduroam safe to use?

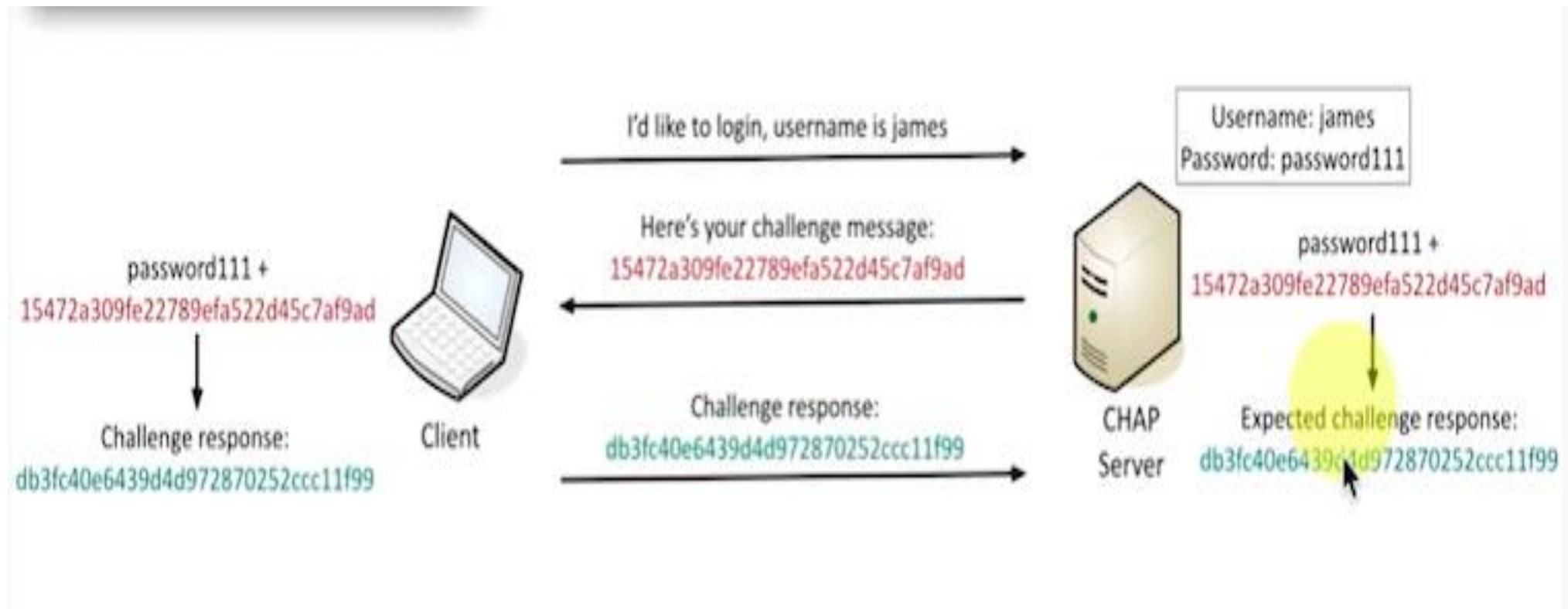
eduroam is based on the most secure encryption and authentication standards in existence today. Its security by far exceeds typical commercial hotspots.

802.1x Authentication (PEAP/TTLS)

- Framework 802.1x:
 - Radius with tunneled EAP (TTLS, PEAP)



MSCHAPv2.0

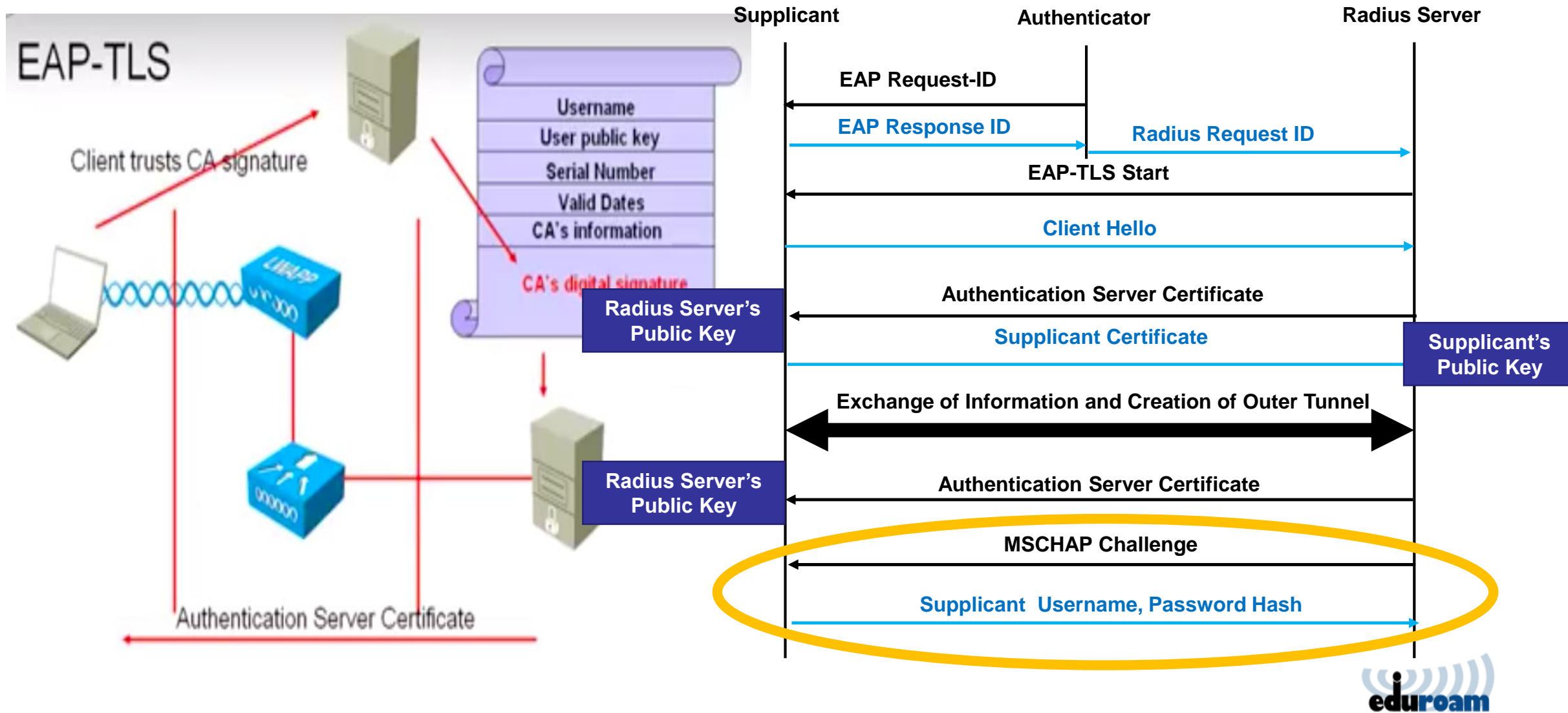


Security of MSCHAPv2.0

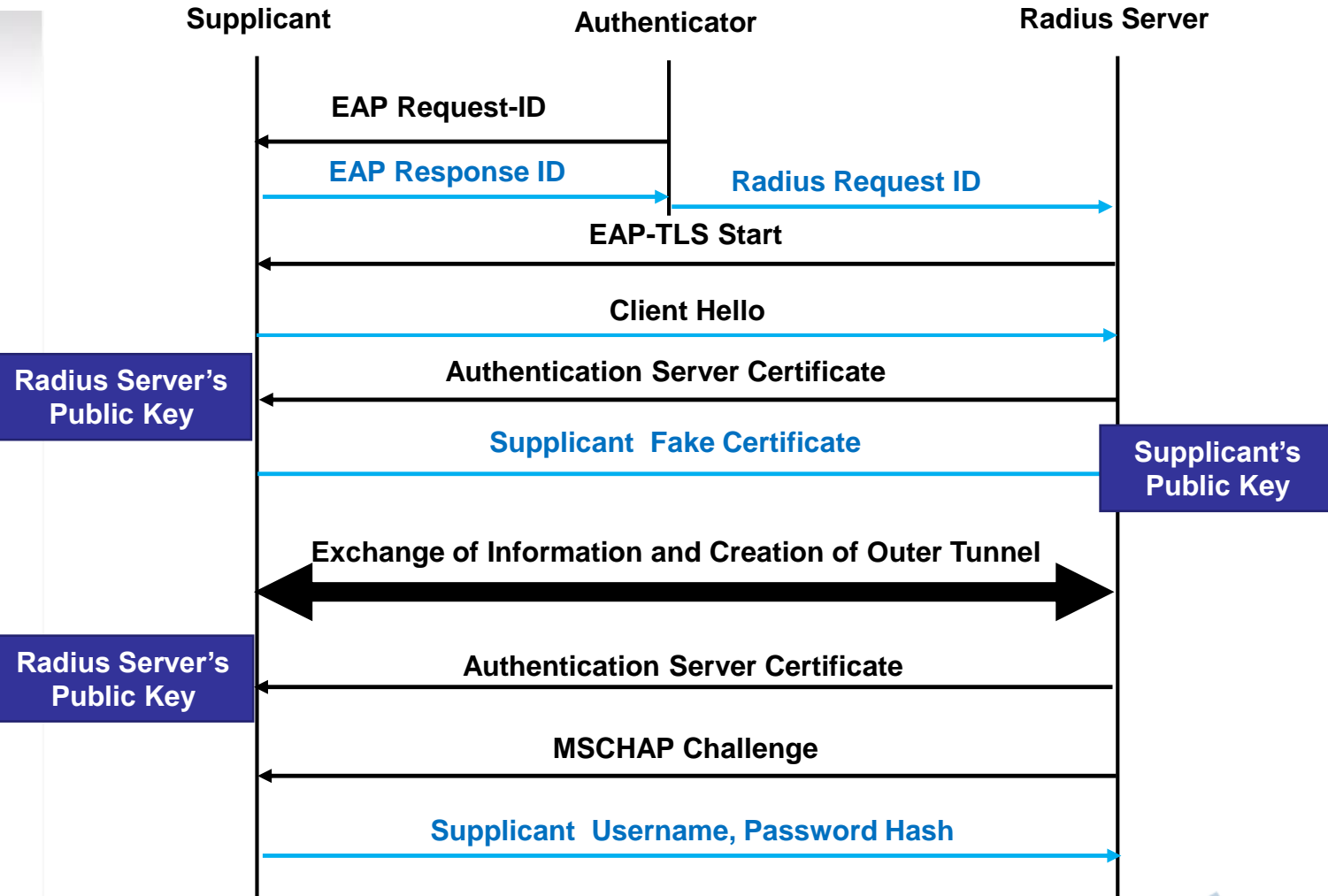
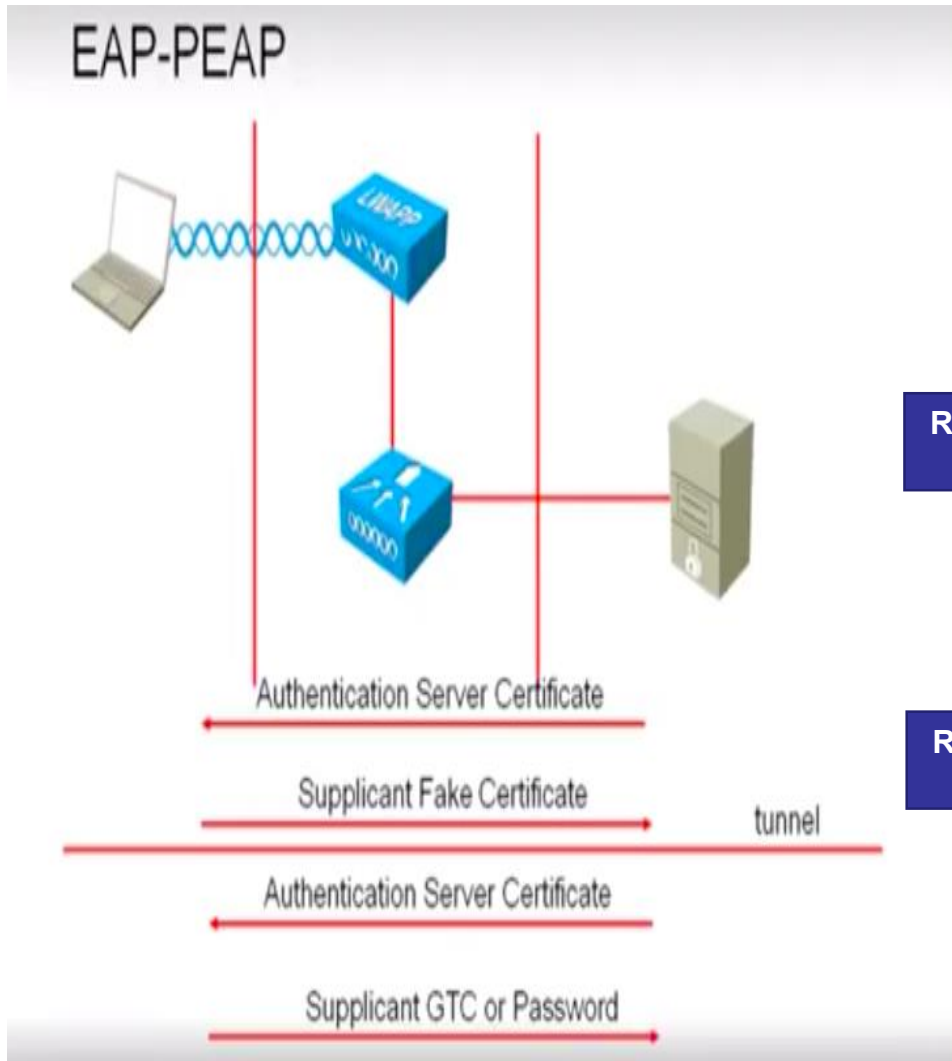
- MSCHAPv2 has been proven weak (broken) back in 1999:
 - 1999: Bruce Schneier: Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)
https://www.schneier.com/academic/archives/1999/09/cryptanalysis_of_mic_1.html
 - Resulted into tools that can brute-force the password from collected challenge-responses.
Most known: **asleep** (http://www.willhackforsushi.com/?page_id=41) (2007)
 - So EAP-PEAP-MSCHAPv2 is only secure if you properly validate the RADIUS server certificate.
- ... Don't worry; it will get worse...



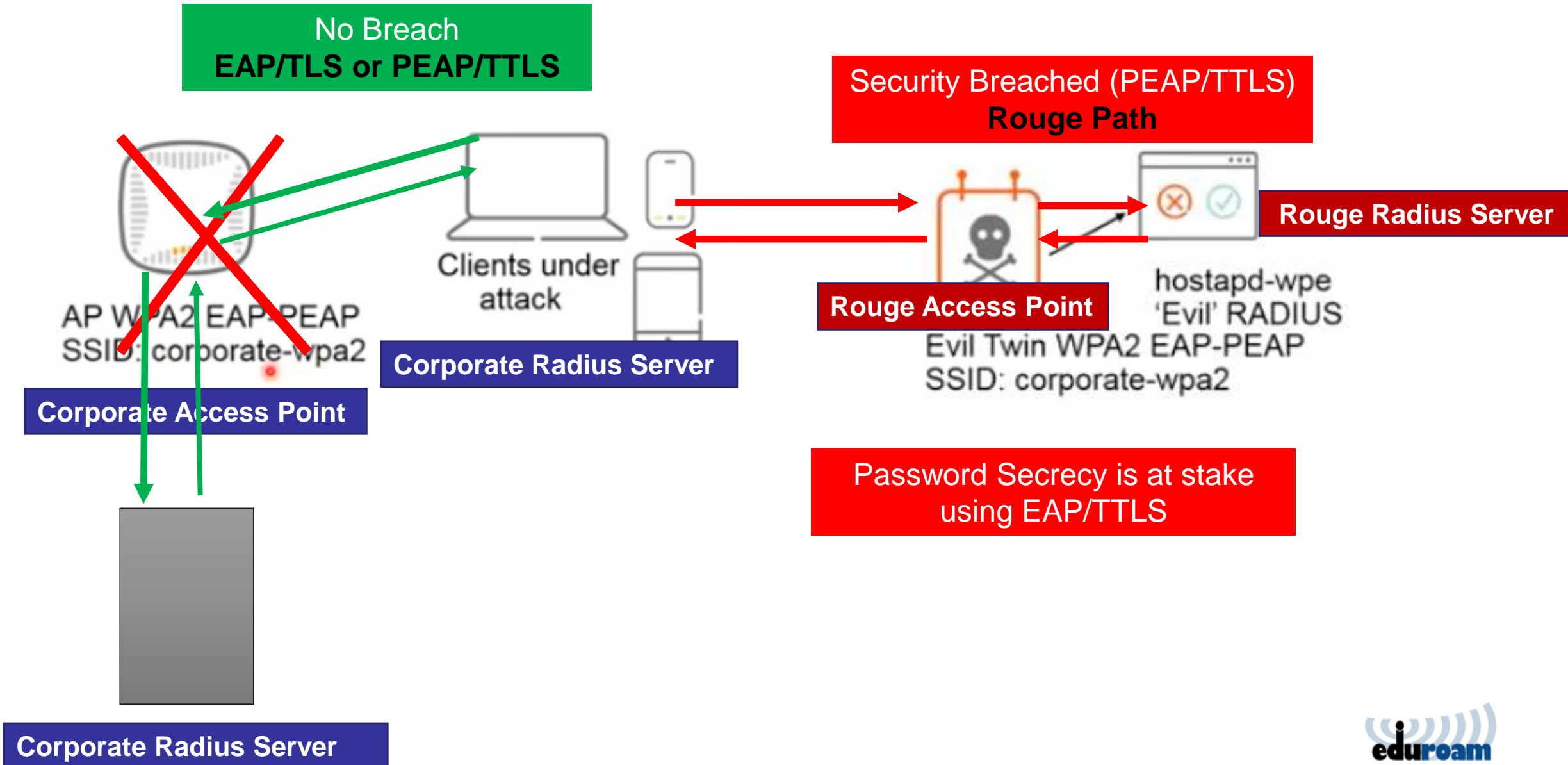
Flow of Authentication EAP-TLS-MSCHAPv2



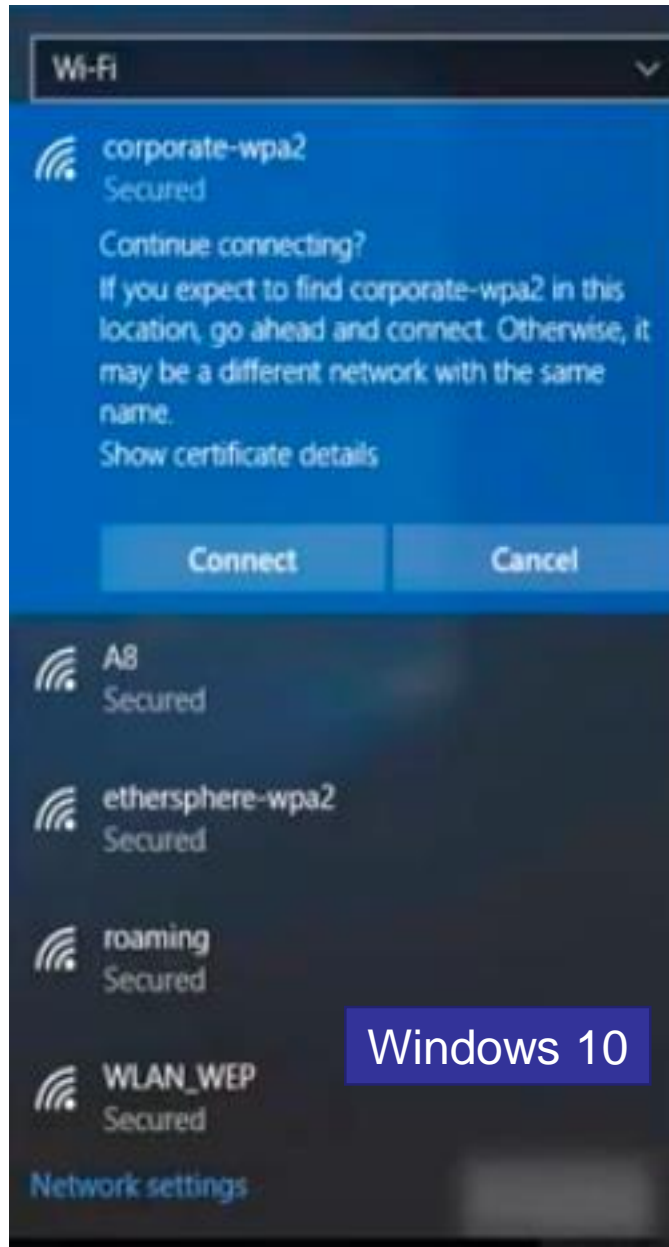
Flow of Authentication EAP-PEAP-MSCHAP



Security Breach?



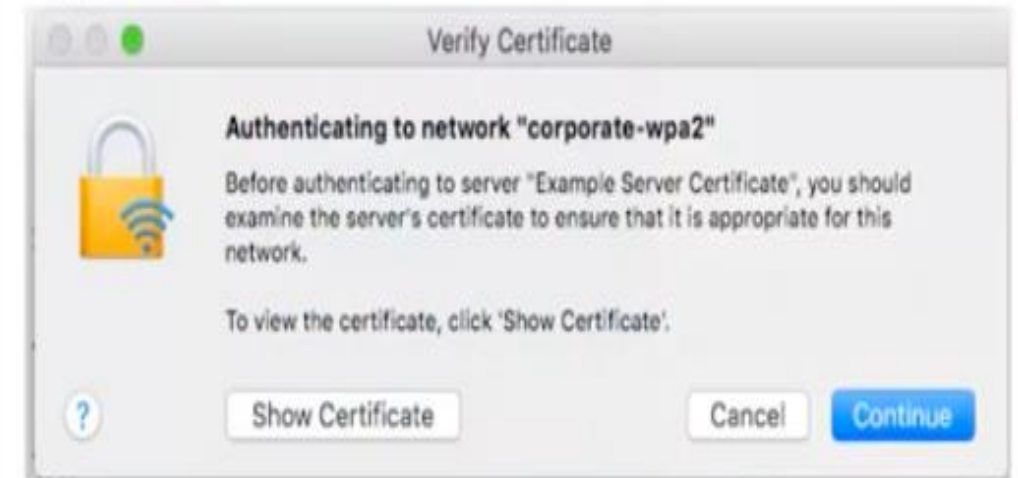
Will supplicants get Warnings?



Windows 10



Windows Phone 8.1



Apple Mac

Will supplicants give Warning?

Continued

Kindle



Android

Apple Mac Book



No warnings of Rouge Server for Kindle, Android and Apple Mac Book

MSCHAPv2 Responses Received by Rouge Radius Server

File hashes4john.txt:

```
win10.doe:$NETNTLM$065b3259a7c38a46$67f05bf1e944ad63033f083dace3bbefb3766e7af8c4805
kindle.doe:$NETNTLM$ad985b8190684861$227dbc2b4978916804d194ae65804fbe70ddd2d578833d30
osx.doe:$NETNTLM$45a2b55b0beac2e5$dec93443784410a3542f1b54e14f9884ea90a012e1dfcdcd
kindle.doe:$NETNTLM$194e46fc539ec008$8d5d9a24432f16f106bd1e2e6940eea73553ebf4d4d221ce
ubuntu.doe:$NETNTLM$c0bb4f56dfe37d73$6c74a501020d32a0aa51f9a1777ed36e9c3a5cebb750f4f4
chromebook.doe:$NETNTLM$7012580be7e072a7$b7637c5192a4013b1e40c6ddbe17657fe9bb5295750e0326
```

<https://www.youtube.com/watch?v=50fO3j4NgyQ> by Herman Robers

How to make it secured: EAP-TLS

Source: https://monitor.eduroam.org/mon_direct.php

- **Option: 1**
 - Use EAP-TLS rather using EAP-TTLS

Problems of using EAP-TLS

- Management Challenge
 - Issuance of Individual Certificates
 - Revoking of Individual Certificates
- Difficult to make it scalable
- Not that popular in Eduroam industry

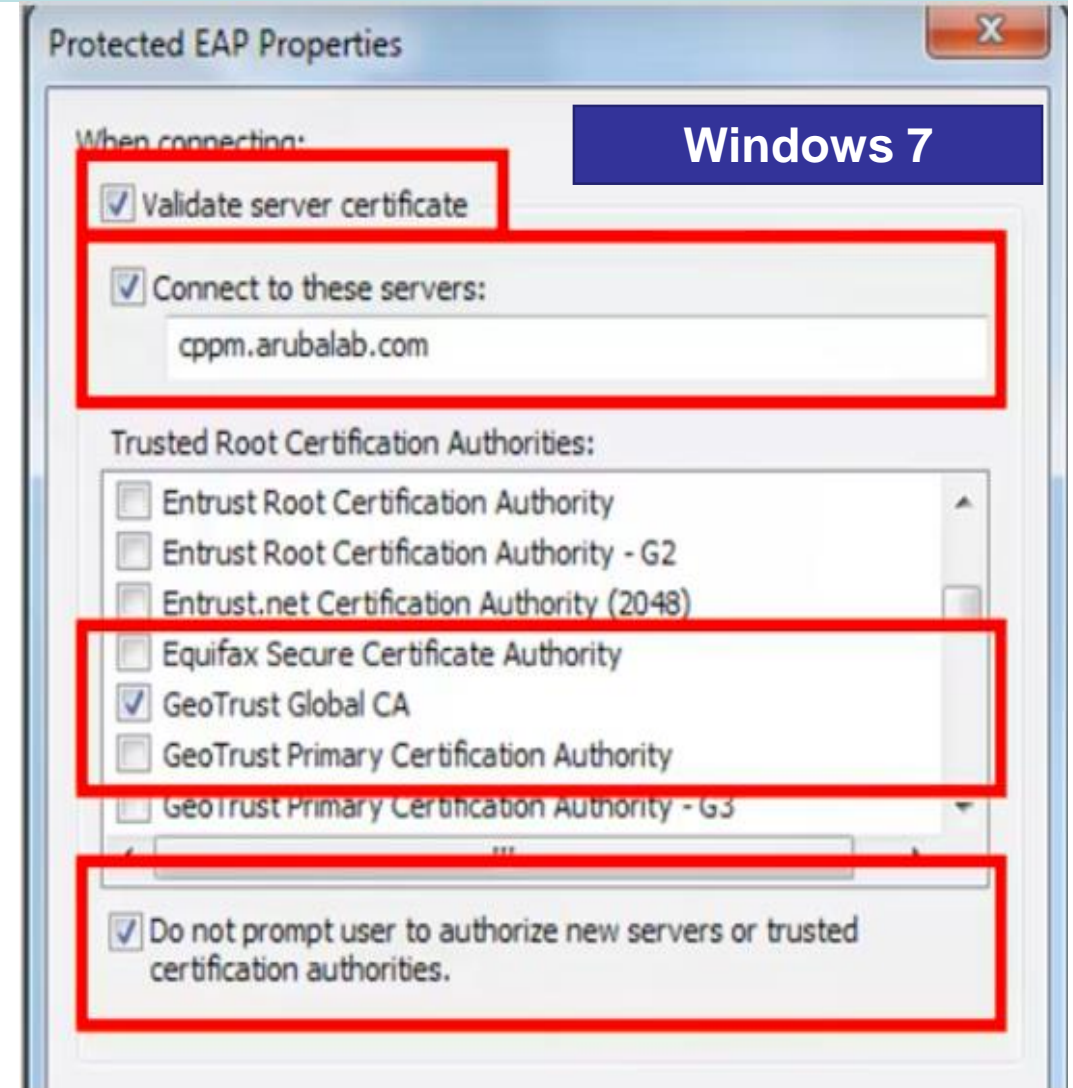
| Level | Server Name | Status | Tested realm | Checked with |
|-------|-----------------|--------|-----------------|--------------|
| ad | RADIUS server 1 | ✓ | eduroam.ad | EAP-TTLS |
| al | RADIUS server 1 | ! | eduroam.al | EAP-TTLS |
| am | RADIUS server 1 | ! | eduroam.am | EAP-TTLS |
| | RADIUS server 2 | ! | eduroam.am | EAP-TTLS |
| at | RADIUS server 1 | ! | eduroam.at | EAP-TTLS |
| | RADIUS server 2 | ✓ | eduroam.at | EAP-TTLS |
| be | RADIUS server 1 | ✓ | eduroam.be | EAP-TTLS |
| | RADIUS server 2 | ✓ | eduroam.be | EAP-TTLS |
| bg | RADIUS server 1 | ✓ | eduroam-test.bg | EAP-TTLS |
| | RADIUS server 2 | ✓ | eduroam-test.bg | EAP-TTLS |
| br | RADIUS server 1 | ✓ | eduroam.br | EAP-TTLS |
| | RADIUS server 2 | ✓ | eduroam.br | EAP-TTLS |
| by | RADIUS server 1 | ✓ | eduroam.by | EAP-TTLS |
| ca | RADIUS server 2 | ✓ | test.eduroam.ca | EAP-TTLS |
| | RADIUS server 3 | ✓ | test.eduroam.ca | EAP-TTLS |
| | RADIUS server 4 | ✓ | test.eduroam.ca | EAP-TTLS |
| | RADIUS server 5 | ✓ | test.eduroam.ca | EAP-TTLS |
| ch | RADIUS server 1 | ✓ | eduroam.ch | EAP-TTLS |

How to make it secured: **EAP-TTLS**

- **Options: 2**

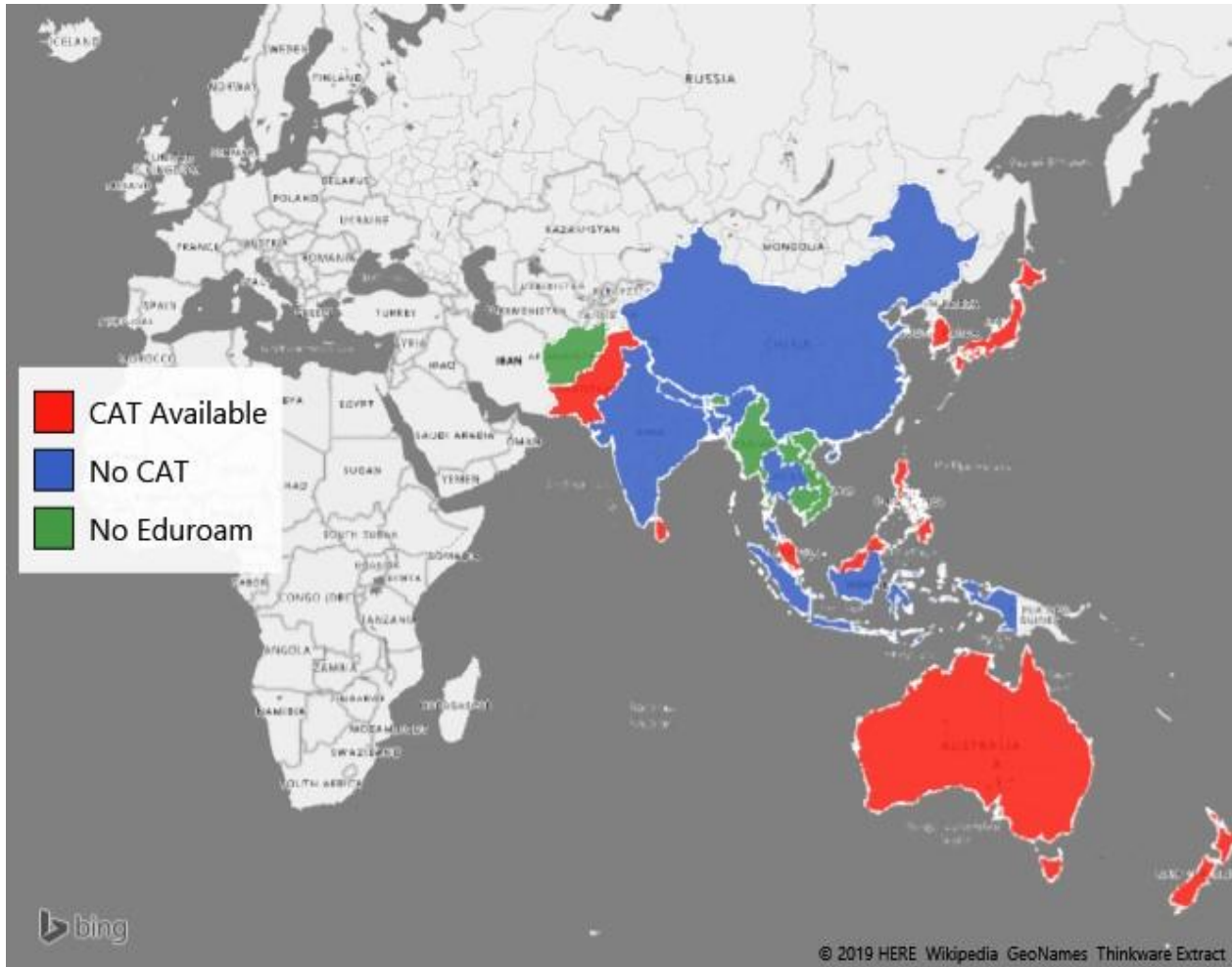
- Follow the Trusted Rules →→→→
 - Applicable for Windows and iOS
 - Disaster for Android, Kindle
- May be difficult for the user to configure

Role of CAT!!!!!!



Availability of CAT

<https://cat.eduroam.org>



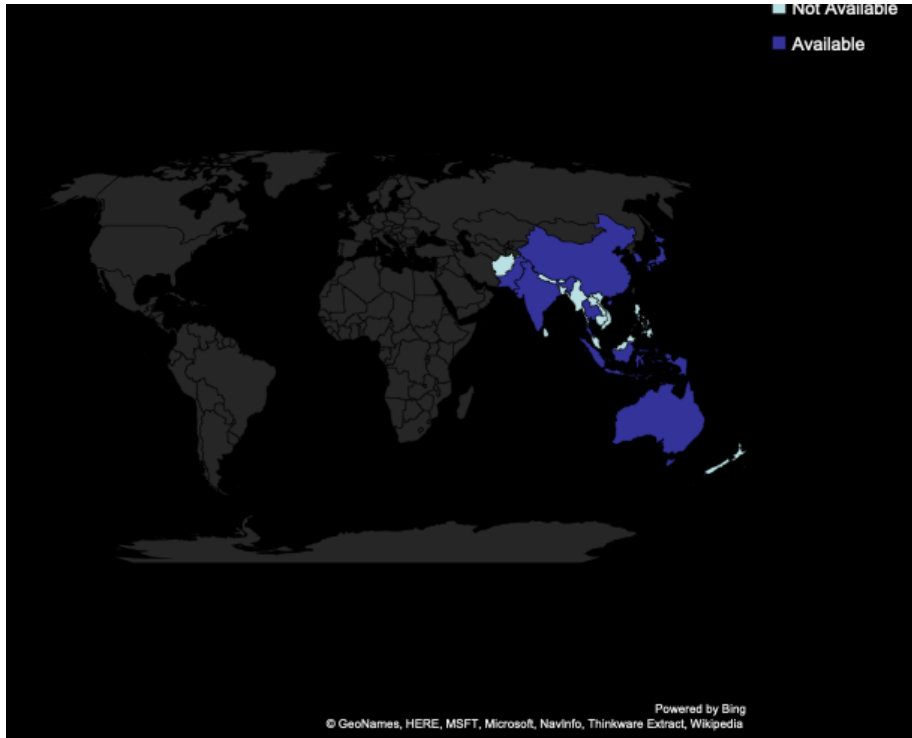
Under Asi@Connect

- CAT Available: 7
- No Eduroam Availability: 6
- CAT Not Available: 11

Among fDLuDCf partners

- Only Sri Lanka and Philippines have CAT services
- Bangladesh, Thailand, Nepal don't have CAT Services
- Bhutan is still under a Pilot Project

Availability of exclusive eduroam webpage



Under Asi@Connect

- Webpage Available: 12
- Webpage not Available: 12

Among fDLuDCf partners

- Only Thailand has exclusive eduroam webpage
- Bangladesh, Nepal, Philippines and Sri Lanka don't have exclusive Webpage
- Bhutan is still under a Pilot Project

Roadmap for BdREN

- Increased Coverage
 - More Universities, Medical
 - Government Organizations
 - ISP Hotspots
 - Libraries, museums, airports
 - Usage:
 - Authentication Statistics
 - Visibility:
 - Make the IdPs, SPs and I
 - Make eduroam hotspots a
- [Source: <https://www.eduroam.org>]



Supporting services



monitor.eduroam.org

Facts (DB) ▾

Maps ▾

Monitoring ▾

Statistics (F-ticks) ▾

Configure your device (CAT)

Login

General information

Important notice for NROs! Deadline for migration to eduroam data base format v.2.0 is November 30, 2019. [More information.](#)

Europe

Africa

APAN

SOAM

NOAM

| Country | NREN/NRO | Number of service locations | Number of IdPs | Number of SPs |
|-----------------|----------|-----------------------------|----------------|---------------|
| Australia | AARNet | 410 | 74 | 93 |
| Bangladesh | BdREN | N/A | N/A | N/A |
| China, Mainland | CSTNET | 3 | 3 | 3 |
| Hong Kong | JUCC | N/A | N/A | N/A |
| India | ERNET | N/A | N/A | N/A |



Roadmap for BdREN

Continued



Supporting services

monitor.eduroam.org

Facts (DB) ▾

Maps ▾

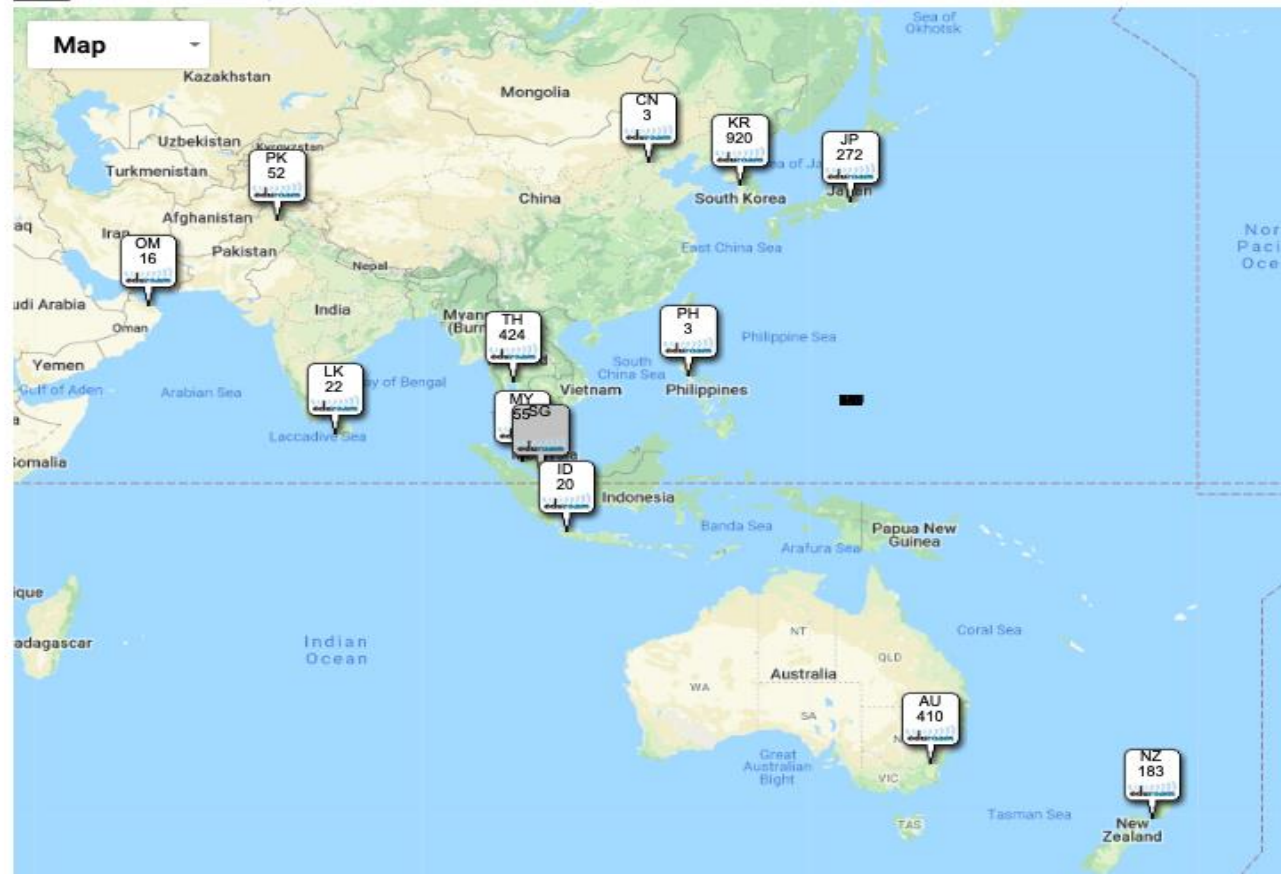
Monitoring ▾

Statistics (F-ticks) ▾

Configure your device (CAT)

Maps

Global < APAN eduroam map



- Visibility Issue:
 - Ensure Presence in EduRoam Map (https://monitor.eduroam.org/map_service_loc.php)







Roadmap for BdREN

Continued

<https://monitor.eduroam.org/index.php>

- 59 countries are there out of 100
- Monitoring
 - Radius Server Monitoring
 - Infrastructure Monitoring
 - Status Monitoring

| Level | Server Name | Status | Tested realm | Checked with | Accept time | Reject Time | Monitored ts | History |
|-------|-----------------|--------|--------------|--------------|-------------|-------------|---------------------|---|
| ad | RADIUS server 1 | ✓ | eduroam.ad | EAP-TTLS | 1125 | 2146 | 2019-12-13 08:15:43 |  Graph |
| al | RADIUS server 1 | ! | eduroam.al | EAP-TTLS | 10065 | 20011 | 2019-12-13 08:38:15 |  Graph |
| am | RADIUS server 1 | ! | eduroam.am | EAP-TTLS | 1691 | 1771 | 2019-12-13 08:19:03 |  Graph |
| | RADIUS server 2 | ! | eduroam.am | EAP-TTLS | 1739 | 1738 | 2019-12-13 08:21:18 |  Graph |
| at | RADIUS server 1 | ! | eduroam.at | EAP-TTLS | 461 | 456 | 2019-12-13 08:12:27 |  Graph |
| | RADIUS server 2 | ✓ | eduroam.at | EAP-TTLS | 447 | 360 | 2019-12-13 08:12:33 |  Graph |
| be | RADIUS server 1 | ✓ | eduroam.be | EAP-TTLS | 879 | 847 | 2019-12-13 08:48:45 |  Graph |
| | RADIUS server 2 | ✓ | eduroam.be | EAP-TTLS | 878 | 843 | 2019-12-13 08:48:52 |  Graph |

Roadmap for BdREN

Continued

- 59 countries are there out of 100
- Statistics
 - Statistics per country
 - Global Table
 - Status Monitoring

Global table

F-ticks statistics - table for all countries from 2019-12-01 00:00:00 to 2019-12-15 00:00:00

🕒 Select different time interval

Accept responses

| Visited Federation ↓ | ↔ Users coming from | | | | | | | | | | | | | | | | | | | | | | |
|-------------------------|---------------------|-----|----|--------|-----|--------|-----|-----|-----|------|--------|----|-----|----|----|----|------|-------|------|----|----|------|-----|
| | al | am | ar | at | au | be | bg | br | by | ca | ch | cl | cn | co | cr | cy | cz | de | dk | ec | ee | es | fi |
| am | | 186 | | | | | | | | | | | | | | | | 1 | | | | | |
| at | | | 12 | 219974 | 393 | 874 | | 165 | | 754 | 2887 | 14 | 188 | 3 | 19 | 28 | 5024 | 16765 | 1079 | | 29 | 3048 | 543 |
| be | | | | 1119 | 54 | 231895 | | 102 | | 453 | 800 | 18 | 203 | | 32 | 19 | 1116 | 5052 | 751 | 50 | 10 | 4849 | 28 |
| bg | | | | 8 | | | 496 | | | | 7 | | | | | | 3 | 24 | | | | | 21 |
| by | | | | | | | | | 539 | | 1 | | 7 | | | | 24 | 38 | | | | | 20 |
| ca | | | | 774 | | | | | | | | | | | | | | | | | | | |
| ch | | | | 6055 | 288 | 3181 | | 391 | | 1444 | 173950 | 77 | 900 | | | | 999 | 21063 | 1130 | 1 | 16 | 2820 | 451 |

Source: https://monitor.eduroam.org/f_ticks_matrix.php?gtype=matrix&country=all&obid=all>ime=2019-12-01%2000:00:00::2019-12-14%2023:59:00

What next?

- Arrange awareness development as well as advisory session for participating countries and other NROs for providing guideline about getting incorporated to Configuration Automation and Monitoring Tools and utilities

Can commercial ISPs do it?

- Challenges:

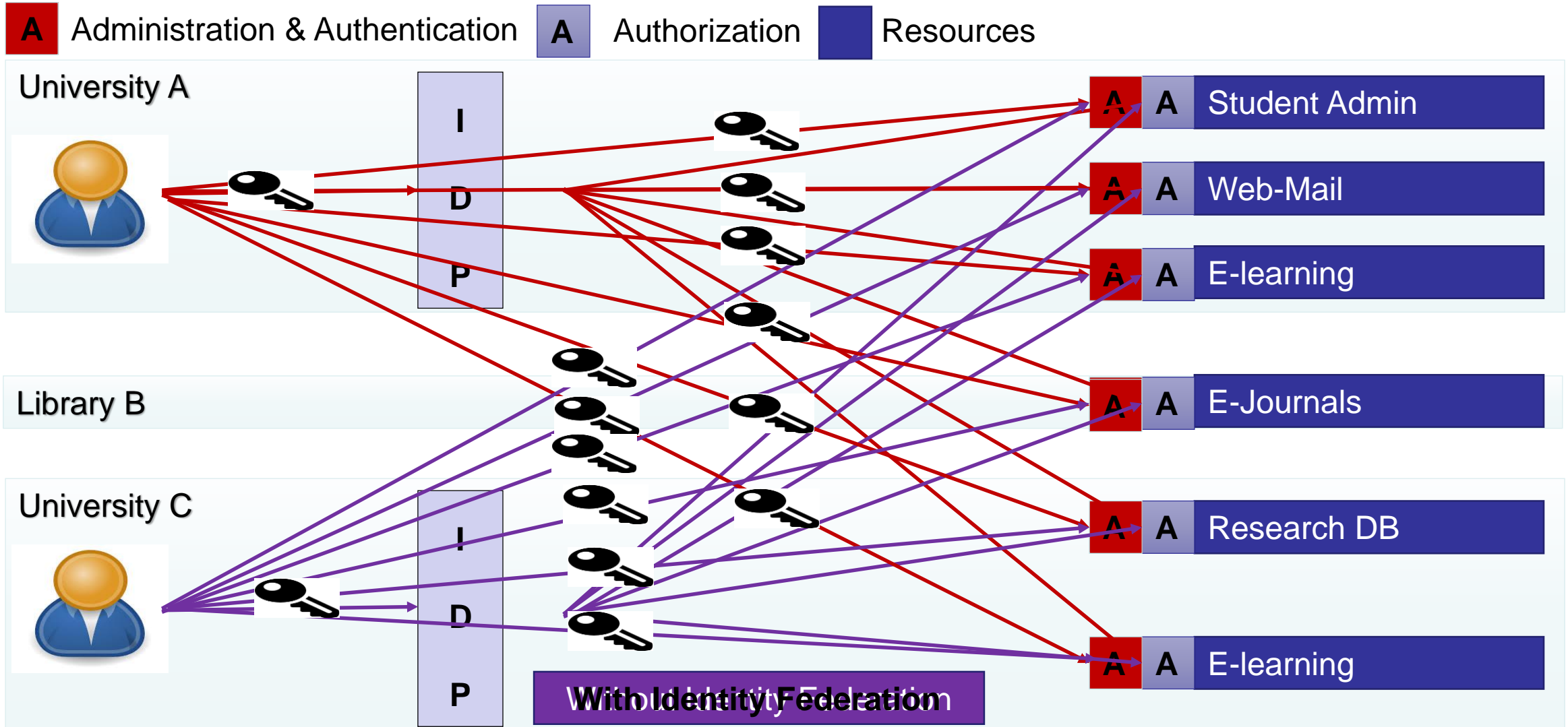
- Routing Radius Request:

- Need an hierarchy same as NRENs
 - IRS → NRS → TLR → eTLR
 - Also can be accomplished by dynamic resolution of RADIUS service from Domain Name Server using SRV record resolution

- Billing:

- Not an NREN concern as NRENs are non-profit organizations
 - A real challenge for ISPs as they need to charge the subscribers

Identity Federation?



Eduroam vs Identity Federation

Is Eduroam synonymous to Federated Identity?

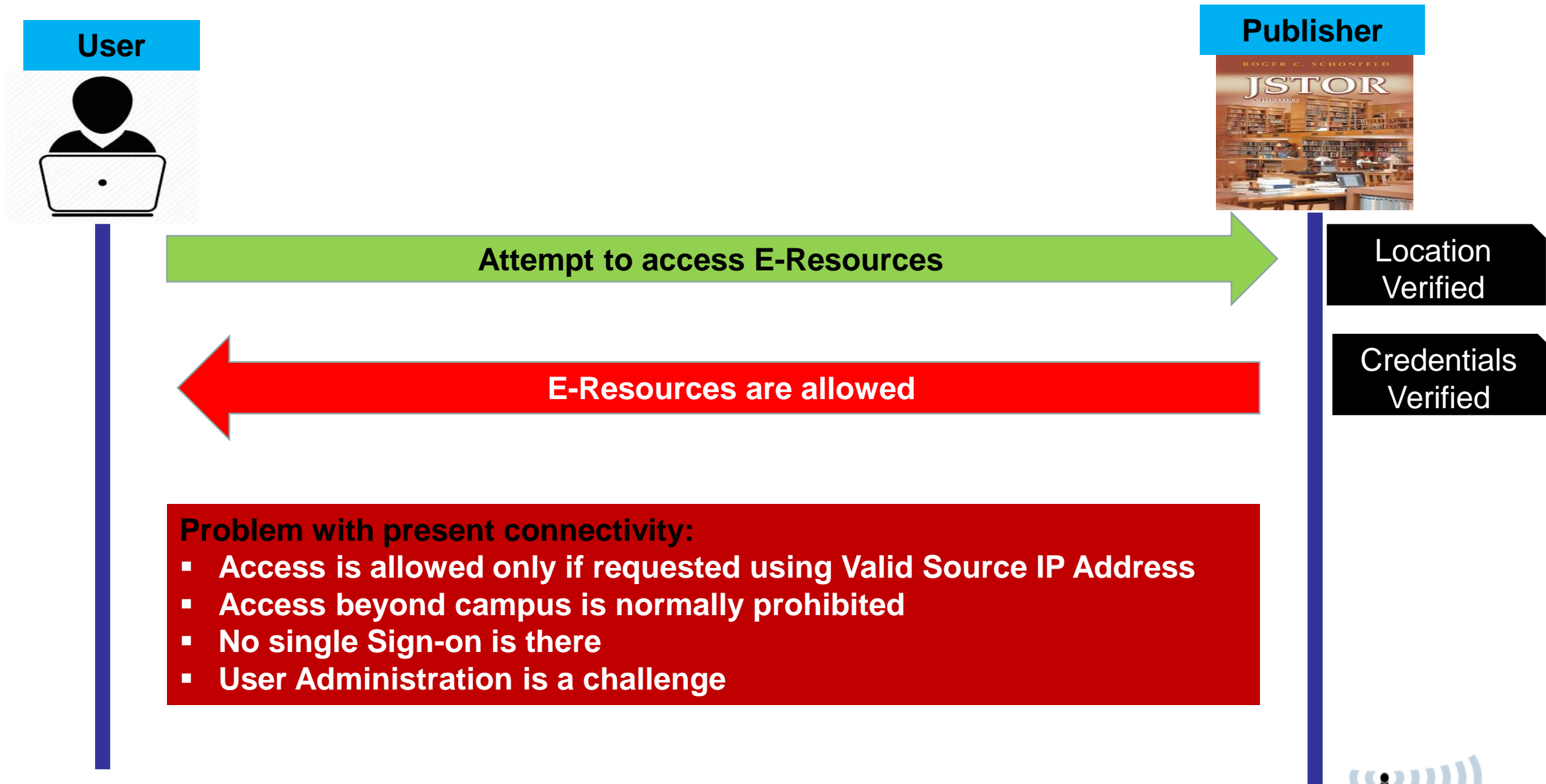
| Eduroam | Identity Federation |
|---|---------------------------------------|
| Authentication is done by Home Server | Authentication is done by Home Server |
| Authentication done using 802.1x | Authentication done using SAML |
| Defined parameters can not be exchanged | Defined parameters are exchanged |
| Credentials Routed by Realm | Credentials sent using WAYF |

Answer is: **Yes and No**
Eduroam is actually a single service Federation

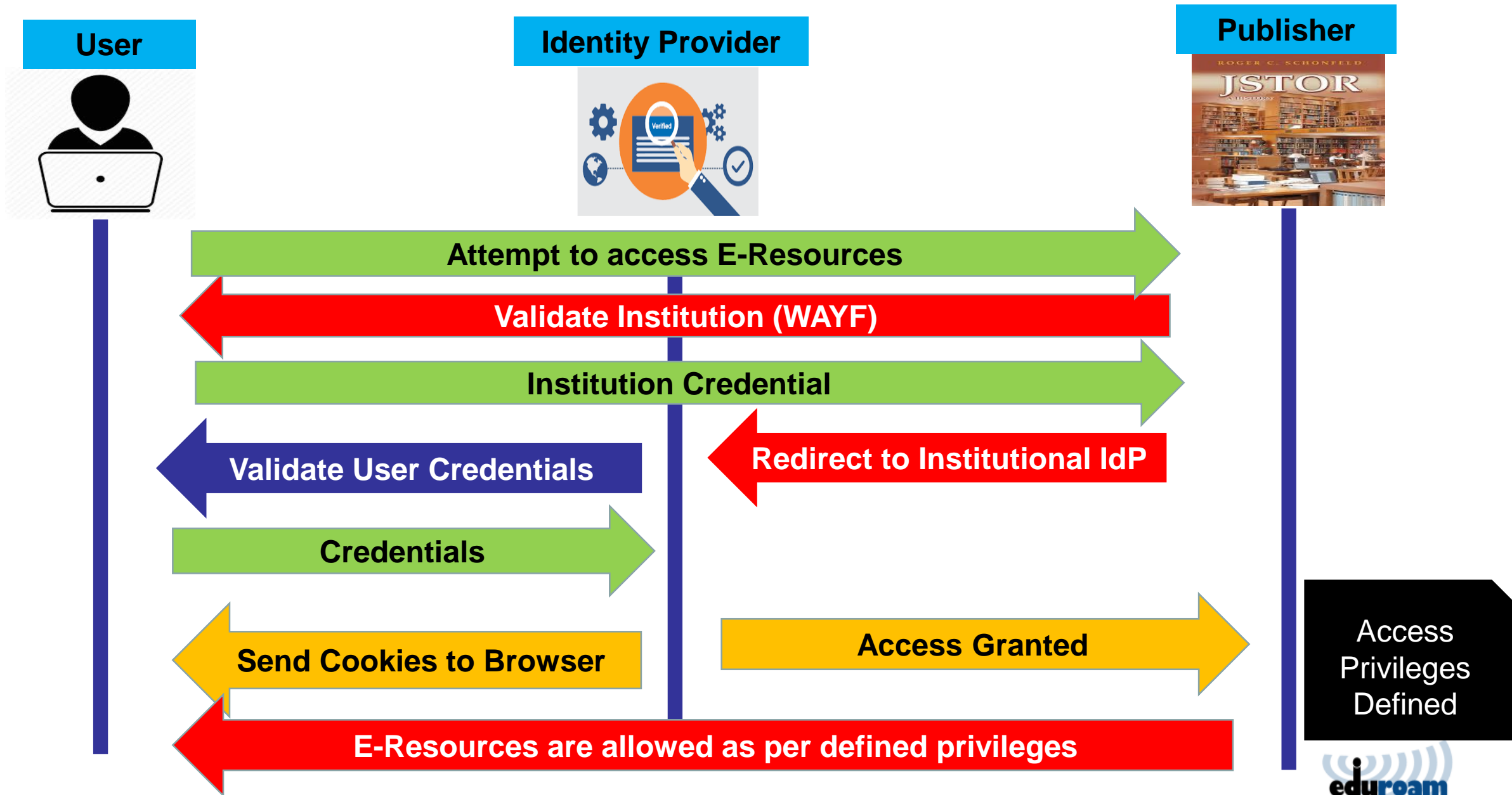
Identity Federation – BdREN Status

- No Federation as of now
- Planning to start
 - HEFED (Higher Education Federation)
- Services Planned
 - Digital Library as a Service (DLaaS)
 - Certificate Management as a Service (CMaaS)
 - Video Conferencing as a Service (VCaaS)

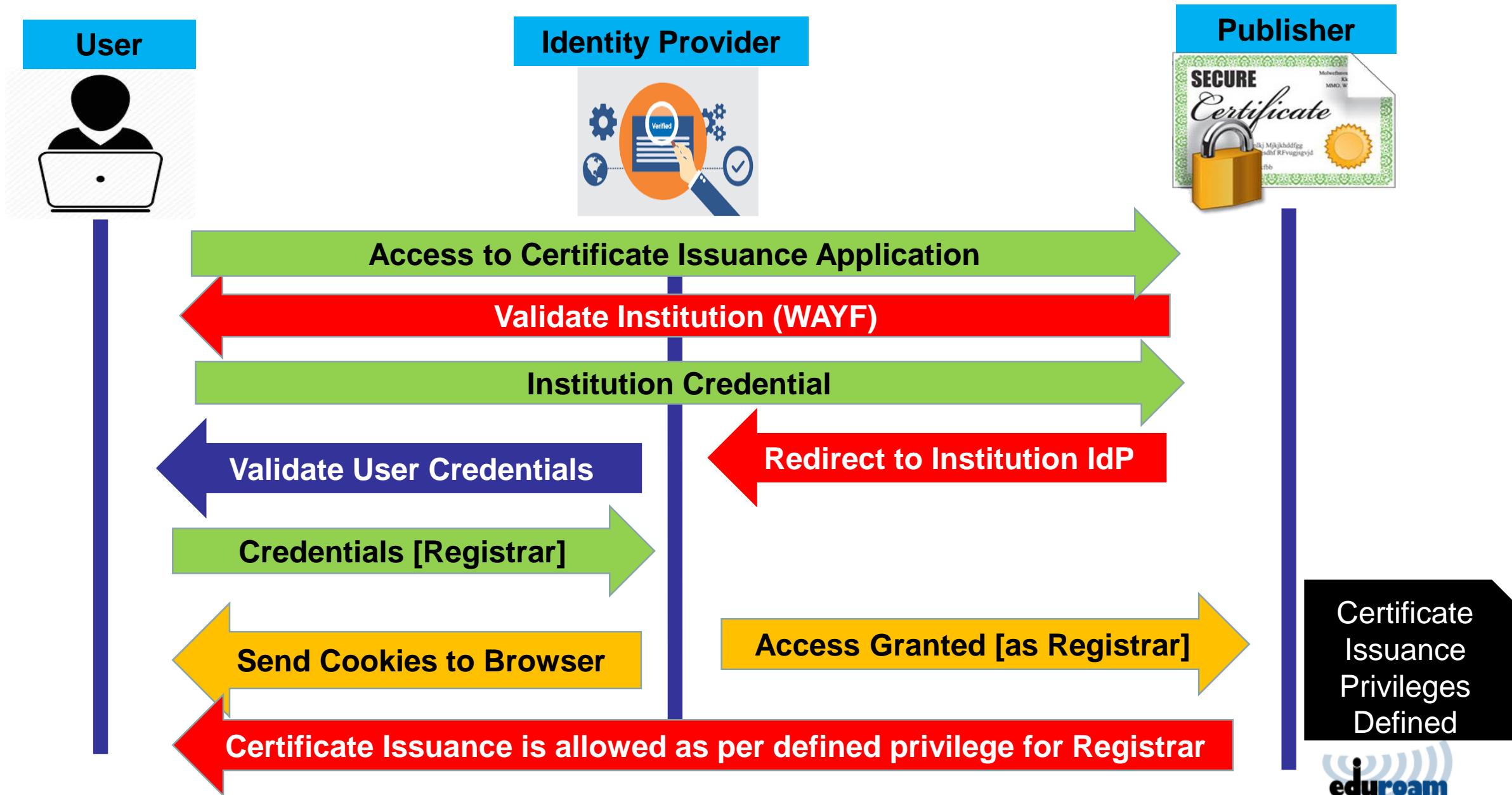
Digital Library, At the moment



Digital Library, Federated Access



Digital Certificate, Federated Access



Roadmap for BdREN, Federated Identity



Creation of Federation



Creation of Services



Creating Awareness

Thank you!

