

# eduroam

Why Institute for Advanced Study  
Joined this Global Secure Wireless  
Initiative  
and Why You Should Too

*The Institute for Advanced Study is one of the world's leading centers for theoretical research and intellectual inquiry. The Institute exists to encourage and support curiosity-driven research in the sciences and humanities –the original, often speculative thinking that produces advances in knowledge that change the way we understand the world.*

**Currently, a permanent Faculty of approximately thirty eminent academics guides the work of the Schools and each year awards fellowships to some two hundred visiting Members, from about one hundred universities and research institutions throughout the world.**



Secure wireless when IAS Scholars travel

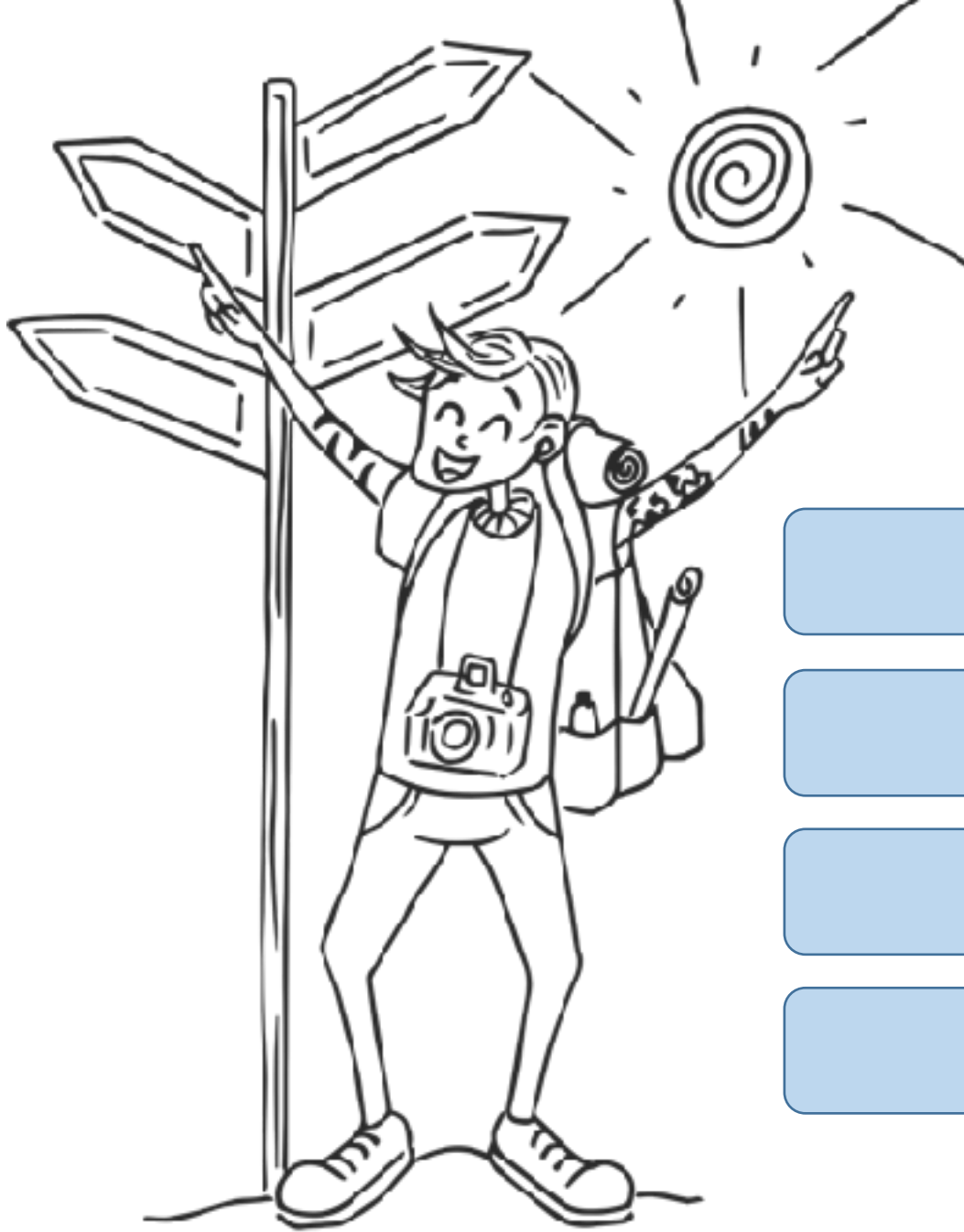
Secure wireless for visitors to IAS campus





## Library resources Princeton University

PU Guest only  
allowed access 1  
week/mo!



What?

Where?

Why?

How?

eduroam (**education roaming**) is the secure, world-wide roaming access service developed for the international research and education community.



eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions by simply opening their laptop.



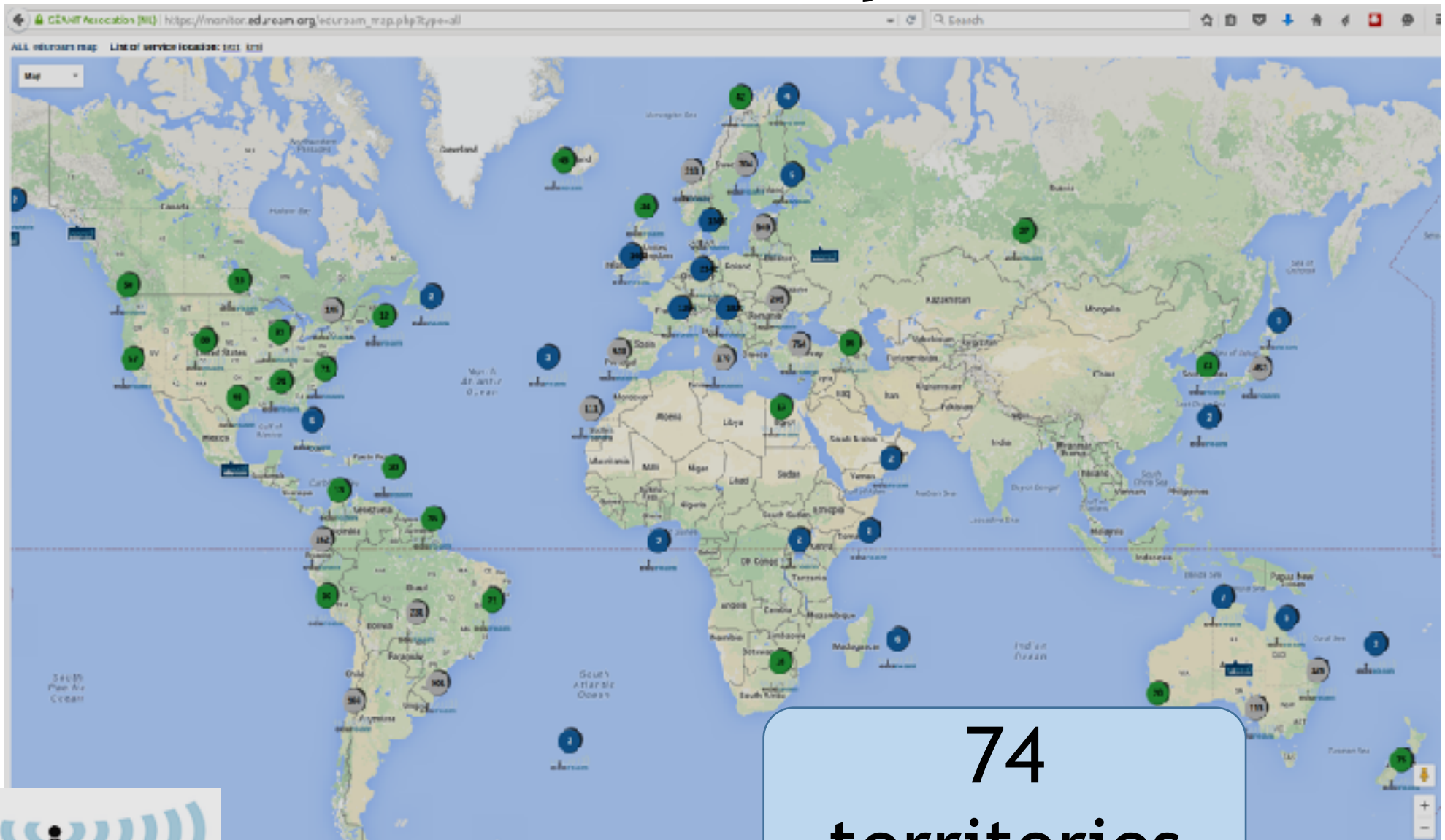
eduroam (education roaming) is the secure, world-wide roaming access service developed for the international research and education community.



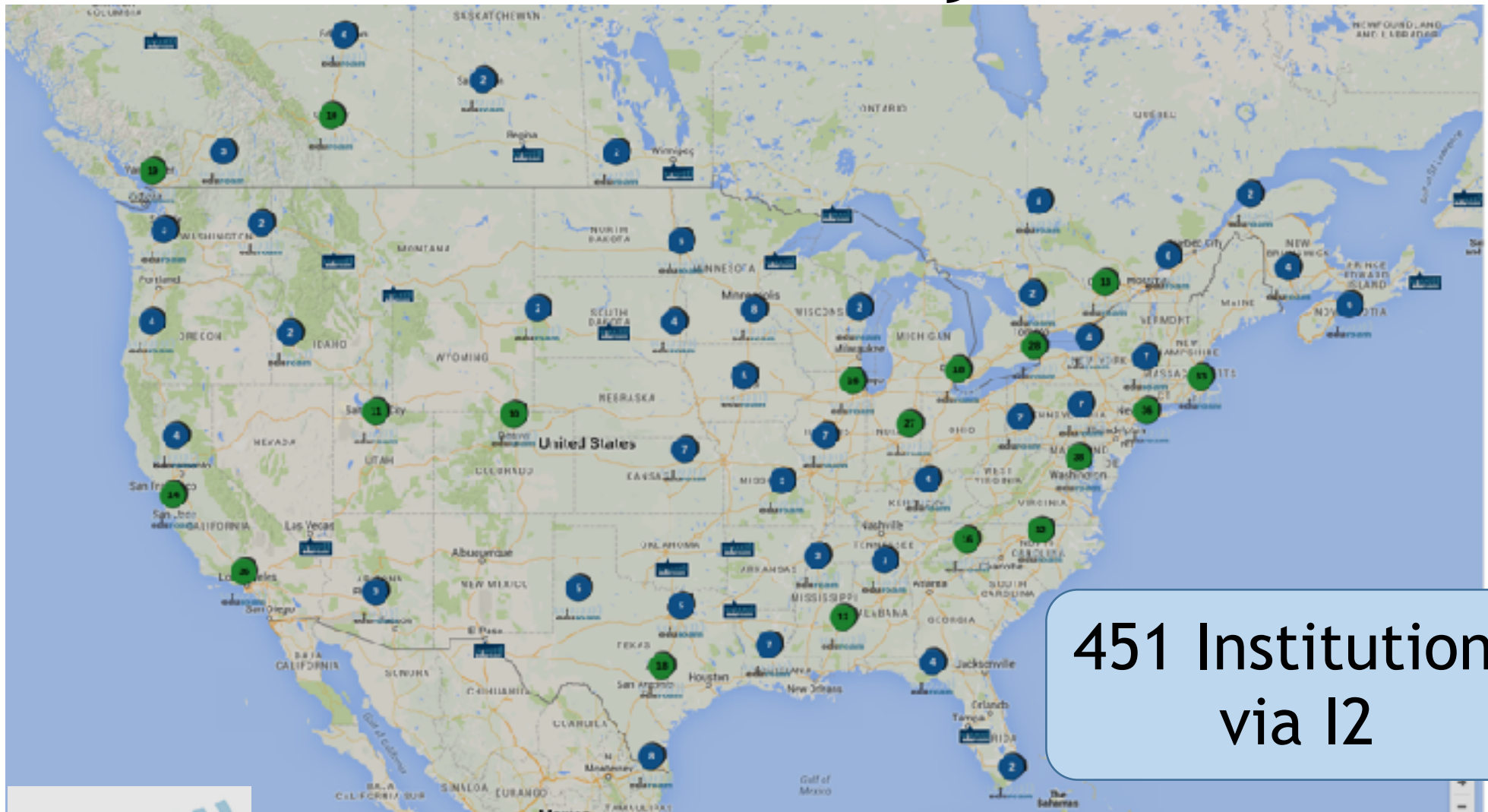
Use your school's Wi-Fi authentication at any eduroam hotspot in the world and join instantly and securely



# Globally



# Nationally



451 Institutions  
via I2

# Regionally

Princeton University

Institute for  
Advanced Study

Rutgers (NB)

Future: Your  
Institution

Future: NJEDge events



3 in NJ


 Institute for Advanced Study



# eduroam user experience

Open laptop/device

Select SSID = eduroam

Connection!



# eduroam - benefits for IT

**Eliminates  
guest  
accounts**

**Can still control  
bandwidth**

**Improves  
security for  
visitors**

**Allows  
access  
resource  
control**

# IT Time Investment

Existing  
802.1X  
SSID?

~2  
Hours

# IT Financial Investment

Cost for  
NJEDge/  
I2  
members

Nada

## 5 Easy Step to Set up eduroam

1. Submit a request to join at [www.eduroam.us](http://www.eduroam.us)
2. Exchange IP address & shared radius secret with eduroam.us
3. Connect your radius server to eduroam-US federation
4. Broadcast a 802.1X ssid called eduroam
5. Advertise the service to your community

# Jargon Alert!

Service  
Provider  
(SP)

Identity  
Provider  
(IDP)

Service  
Provider

Broadcasting SSID  
eduroam

Configured eduroam access  
to internet

Forwarding radius request  
up eduroam chain

Can be any organization

## Identity Provider

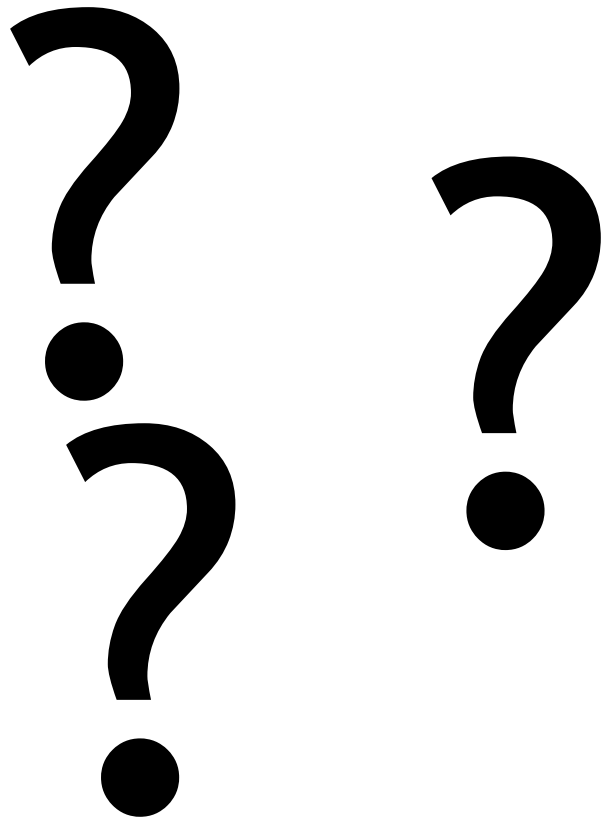
Peers with eduroam radius  
servers

Radius connects to directory  
services

Authenticate user's  
credentials

Can only be academic institution

# No Radius



Service Provider

~~Identity Provider~~

[user@ias.edu](#) on IAS Campus

IAS

Service  
Provider  
(SP)

Identity  
Provider  
(IDP)

user@ias.edu on Princeton U

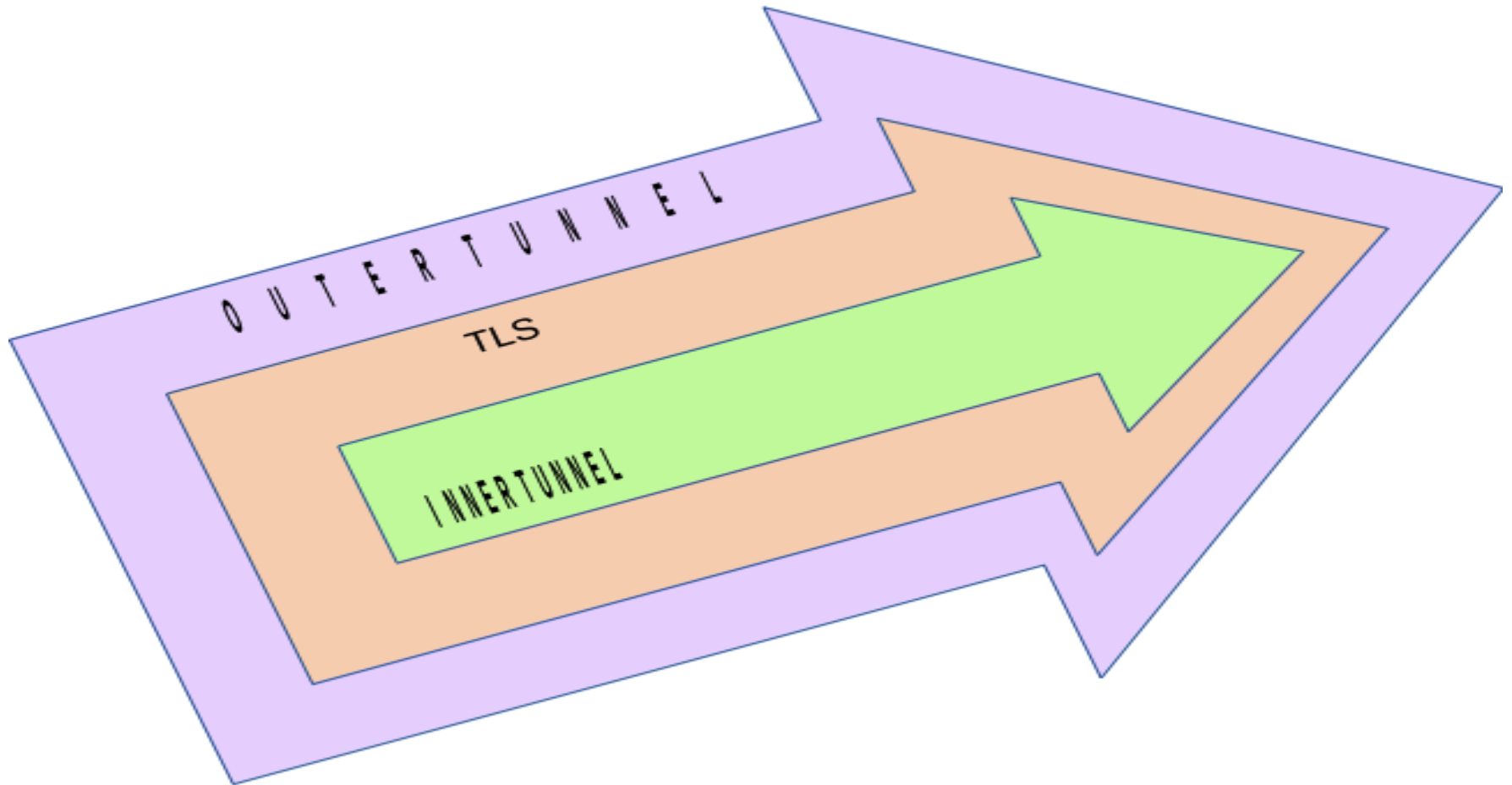
Princeton University

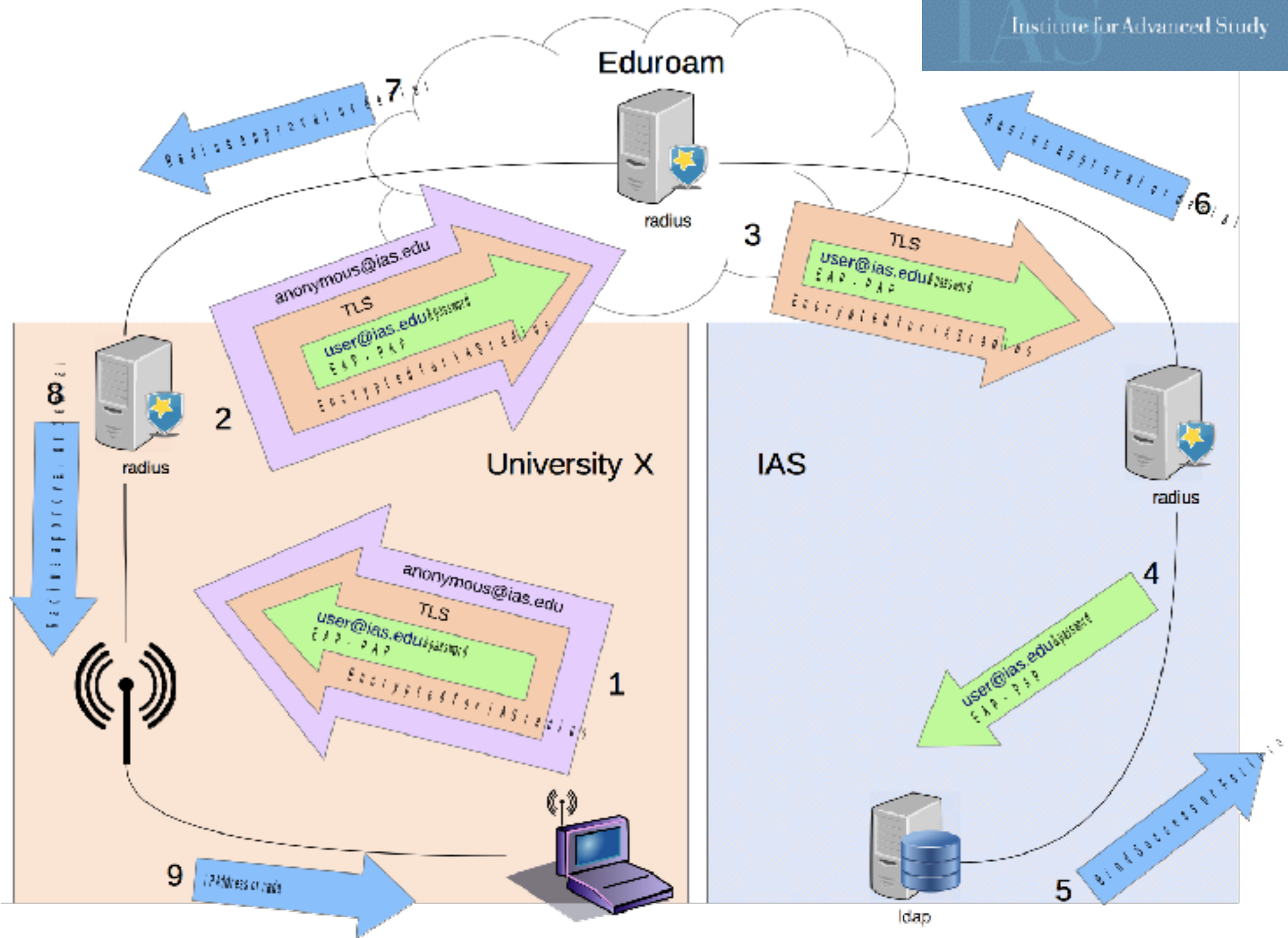
Service  
Provider  
(SP)

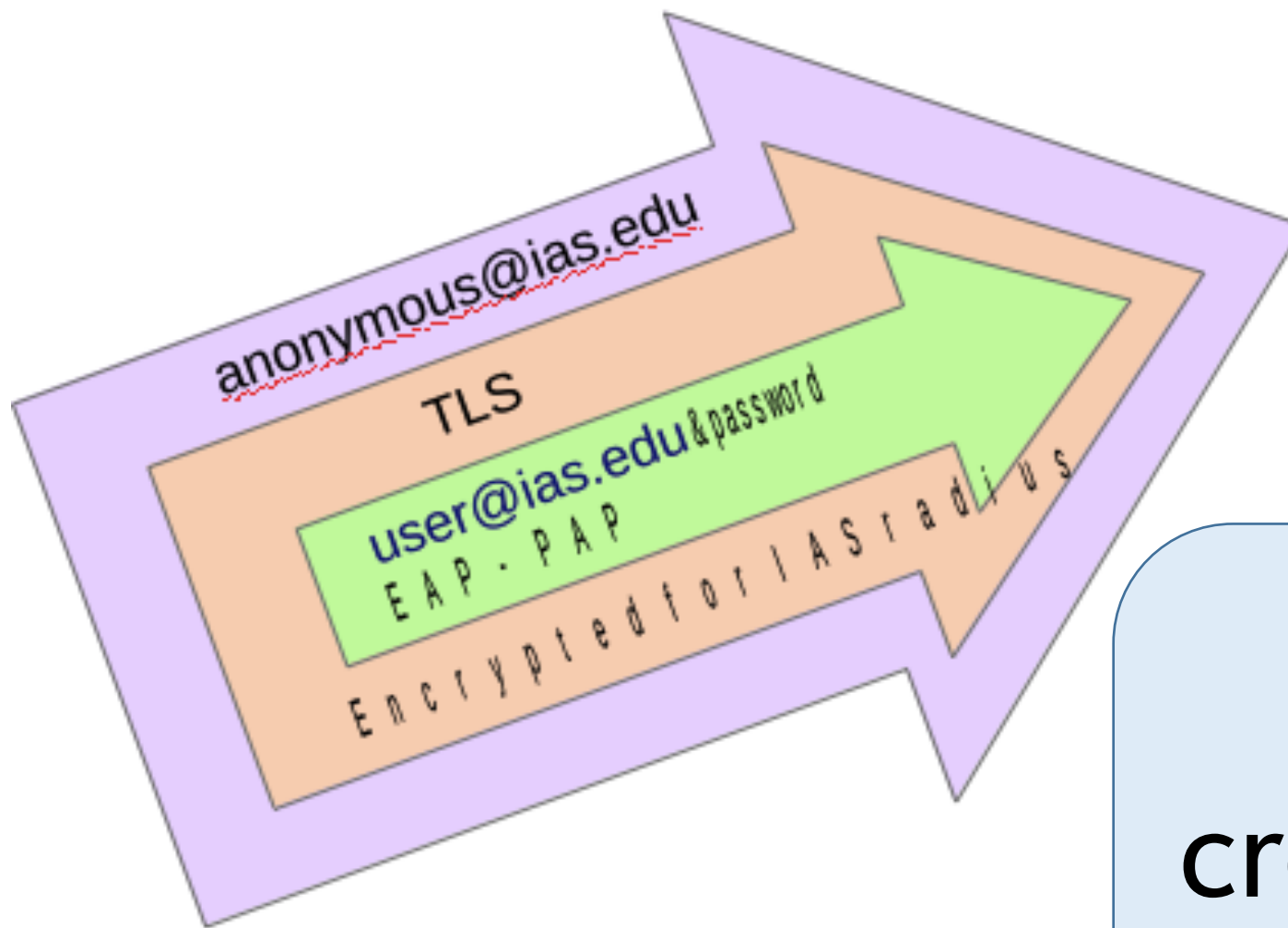
IAS

Identity  
Provider  
(IDP)

eduroam is a federation of radius servers







User  
credentials  
are never  
seen by SP

# Implementation

Create a new radius pool for  
eduroam.us radius servers

Exchange radius secrets with  
eduroam.us

Broadcast 802.X SSID called  
eduroam

Add eduroam to 802.1X provisioning  
tool

# Adding eduroam to radius

# Creating eduroam server pool in FreeRadius

```
home_server_pool eduroam {  
    type                = fail-over  
    home_server = tlrs1.eduroam.us  
    home_server = tlrs2.eduroam.us  
}
```

# Configuring the user device

**eduroam Configuration  
Assistant Tool (CAT)**

**<https://cat.eduroam.edu>**

# Configuring CAT

← CEANT Association (NL) | https://cat.eduroam.org

CAT was recently upgraded to version 1.1.1. Please report any issues to the mailing list: cat-users@ceant.net

## Welcome to eduroam CAT

### eduroam Configuration Assistant Tool

View this page in: [Burmese](#) [Català](#) [Čeština](#) [Deutsch](#) [English \(GB\)](#) [Español](#) [Français](#) [Galego](#) [Hrvatski](#) [Italiano](#) [Norsk](#) [Polski](#) [Slovenčina](#) [Slovenski](#) [Svenska](#) [Tagalog](#) [Türkçe](#) [Українська](#) [Magyar](#) [Português](#) [Slovenščina](#) [Start page](#)

[About eduroam](#)

[About eduroam CAT](#)

[Terms of use](#)

[FAQ](#)

[Report a problem](#)

[Become a CAT developer](#)

[eduroam admins manage your IdP](#)

#### eduroam admins: manage your IdP

You must have received an invitation from your national eduroam operator before being able to manage your institution. If that is the case, please continue and log in.

[Log in](#)

#### EAP details for all users

[Add new option](#)

#### eduroam


eduGAIN Social Networks Experimental

Facebook

Google

LinkedIn

Twitter





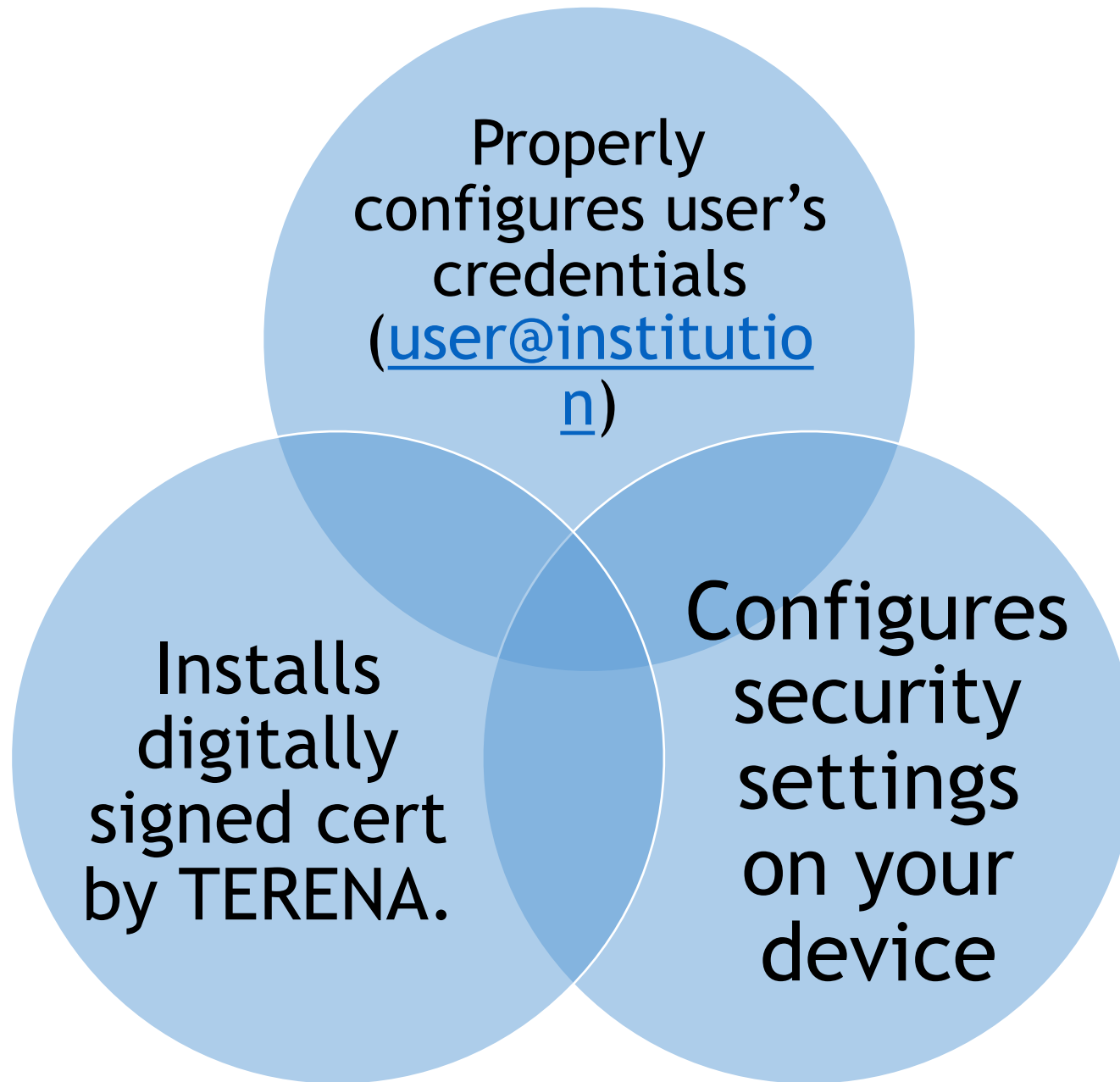
**Choose an installer to download**

	MS Windows 10	<i>i</i>
	MS Windows 8, 8.1	<i>i</i>
	MS Windows 7	
	MS Windows Vista	
	Apple OS X El Capitan	<i>i</i>
	Apple OS X Yosemite	<i>i</i>
	Apple OS X Mavericks	<i>i</i>
	Apple OS X Mountain Lion	<i>i</i>
	Apple OS X Lion	<i>i</i>
	Apple iOS mobile devices (iOS 7 and above)	<i>i</i>
	Apple iOS mobile devices (iOS 5 and 6)	<i>i</i>
	Linux	<i>i</i>
	Chrome OS	<i>i</i>
	Android 6.0 Marshmallow	<i>i</i>
	Android 5.0 Lollipop	<i>i</i>
	Android 4.4 KitKat	<i>i</i>
	Android 4.3	<i>i</i>
	EAP config	<i>i</i>

# CAT isn't a WPA2 supplicant



**MS Windows7 and Vista do not come with a WPA2 supplicant**



Reduce  
Help  
Desk  
Calls

eduroam is  
a  
federation  
built on  
Trust





**Are you sure you want to install profile "eduroam"?**

**Compliance with this policy**

All users of the Institute's information technology resources are expected to comply with the terms of the Institute's Computing Policy.

Regardless of where a user is located or how they are connecting to IAS information technology resources, all users are expected to use these resources in an ethical, respectful and responsible fashion. All users that make use of IAS information technology resources are governed by IAS policies and guidelines as well as all local, state, federal and international laws.

By using this resource, you agree to the terms stated in this web page <http://www.ias.edu/campus/computing/privacy-policy>

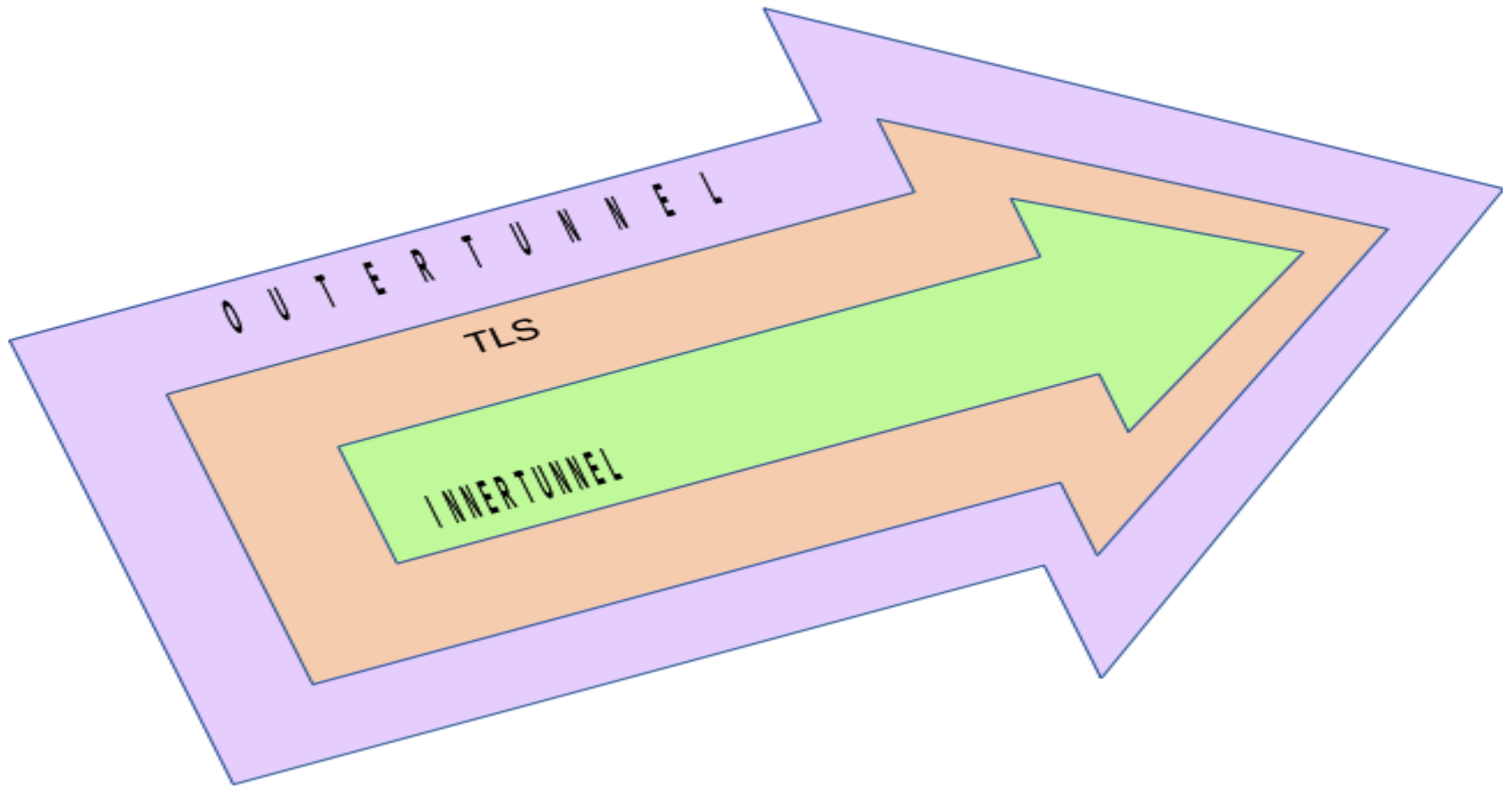
Cancel

Install



All eduroam users have signed an user compliance statement

eduroam is a federation of radius servers



# Outer Tunnel

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons. A filter box is present with the text "Filter:" and a dropdown arrow. To the right of the filter box are buttons for "Expression...", "Clear", and "Apply".

The main display area shows a list of captured packets. The columns are No., Time, Source, Destination, Protocol, and Length. The packets are as follows:

No.	Time	Source	Destination	Protocol	Length
1	2015-11-17 22:32:25.592	Cisco 5a:ab:6a	Cisco 5a:ab:6a	LOOP	68
2	2015-11-17 22:32:30.745	192.168.0.50	64.57.22.74	RADIUS	252
3	2015-11-17 22:32:30.986	64.57.22.74	192.168.0.50	RADIUS	106

The packet list shows that packet 2 is a RADIUS request from 192.168.0.50 to 64.57.22.74, and packet 3 is the corresponding RADIUS response from 64.57.22.74 to 192.168.0.50.

The packet details pane for packet 3 (RADIUS) is expanded, showing the following information:

- Packet identifier: 0x2a (42)
- Length: 210
- Authenticator: b0969b7f08729e109ac645e06ca57dfe
- [\[The response to this request is in frame 3\]](#)
- Attribute Value Pairs
  - AVP: l=19 t=User-Name(1): anonymous@ias.edu
  - AVP: l=6 t=Framed-MTU(12): 1400
  - AVP: l=24 t=Called-Station-Id(30): 54ae.0c57.d4a0:eduroam
  - AVP: l=16 t=Calling-Station-Id(31): 10bf.4806.aaa6

The status bar at the bottom indicates: Frame (frame), 252 bytes; Packets: 68 · Displaye...; Profile: Default.

# Inner Tunnel TLS

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons. A filter bar shows 'Filter:' followed by a dropdown arrow, 'Expression...', 'Clear', 'Apply', and 'Save'. The packet list pane shows two packets:

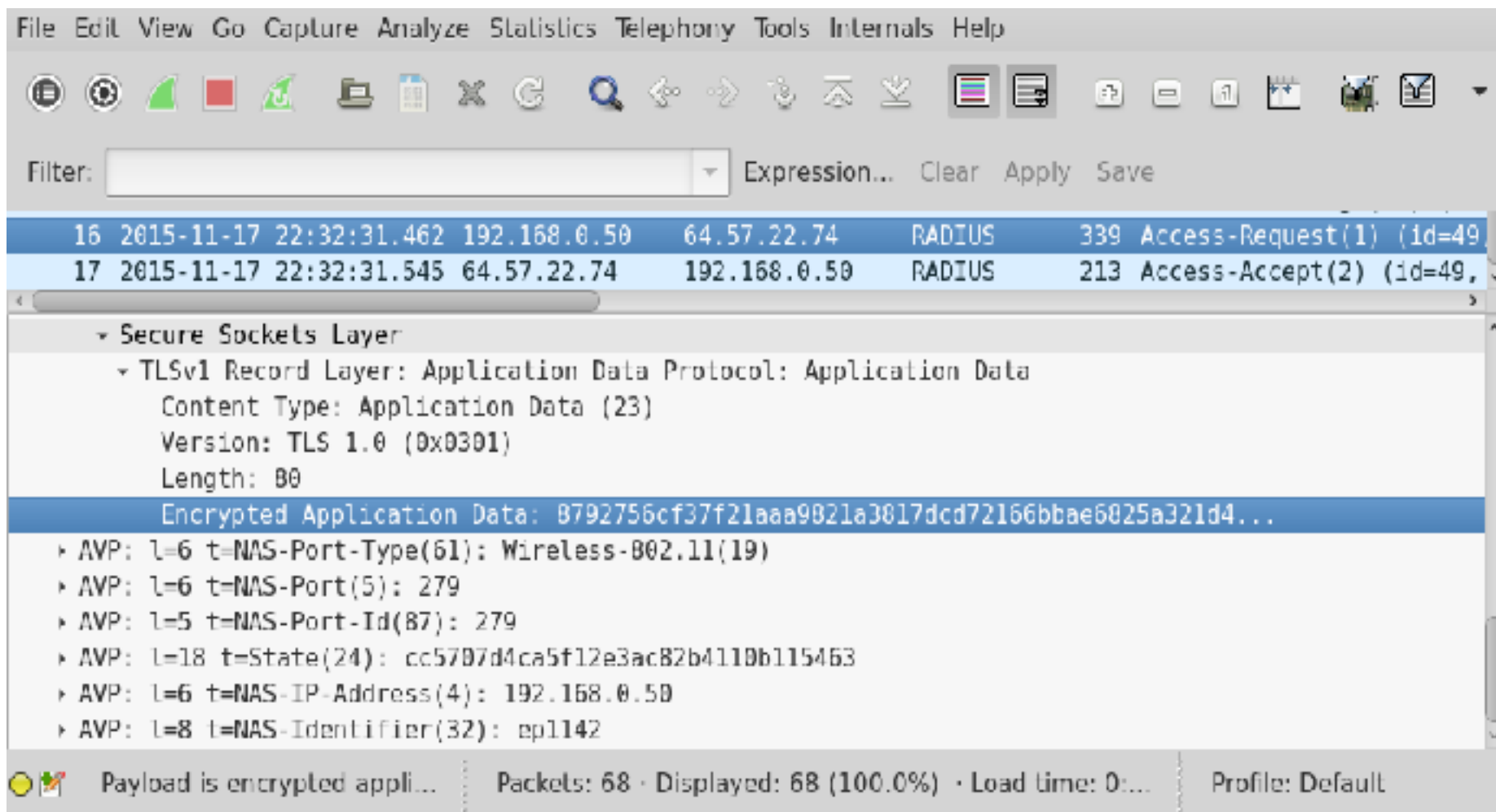
No.	Time	Source	Destination	Protocol	Length	Info
7	2015-11-17 22:32:31.130	64.57.22.74	192.168.0.50	RADIUS	1132	Access-Challenge(11) (id=...)
8	2015-11-17 22:32:31.142	192.168.0.50	64.57.22.74	RADIUS	254	Access-Request(1) (id=45, ...)

The packet details pane for packet 8 shows the following structure:

- Handshake Type: Certificate (11)
  - Length: 3042
  - Certificates Length: 3039
    - Certificates (3039 bytes)
      - Certificate Length: 1282
        - Certificate (pkcs-9-at-emailAddress=network@ias.edu,id-at-commonName=radius.ias.edu,id-at-c...)
          - Certificate Length: 1751
        - Certificate (id-at-commonName=IAS Certificate Authority,pkcs-9-at-emailAddress=network@ias...)
      - TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
      - TLSv1 Record Layer: Handshake Protocol: Server Hello Done
    - AVP: l=18 t=Message-Authenticator(80): 085db9a55a49a733494968d5d6b0c09b

The status bar at the bottom shows: Text item (text), 253 bytes | Packets: 68 · Displayed: 68 (100.0%) · Load time: 0:... | Profile: Default

# Inner Tunnel TLS Credentials



The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons. A filter box is present with the text "Filter:" and a dropdown menu. The packet list shows two packets: packet 16 (Access-Request(1) (id=49)) and packet 17 (Access-Accept(2) (id=49)). Packet 17 is selected, and its details pane is expanded. The details pane shows the following structure:

- Secure Sockets Layer
  - TLSv1 Record Layer: Application Data Protocol: Application Data
    - Content Type: Application Data (23)
    - Version: TLS 1.0 (0x0301)
    - Length: 80
    - Encrypted Application Data: 8792756cf37f21aaa9821a3817dcd72166bbæ6825a321d4...
  - AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
  - AVP: l=6 t=NAS-Port(5): 279
  - AVP: l=5 t=NAS-Port-Id(87): 279
  - AVP: l=18 t=State(24): cc5707d4ca5f12e3ac82b4110b115453
  - AVP: l=6 t=NAS-IP-Address(4): 192.168.0.50
  - AVP: l=8 t=NAS-Identifier(32): ep1142

The status bar at the bottom shows: Payload is encrypted appli... Packets: 68 · Displayed: 68 (100.0%) · Load time: 0:... Profile: Default

# 802.1X Encryption: EAP

EAP-Type	Native Supplicant Support	Pros	Cons
EAP-TLS	Windows (XP, Vista, 7), Mac OS X, Linux, iOS (iPhone, iPod Touch, iPad), Android (v1.6+)	<ul style="list-style-type: none"> <li>Validates client as well as infrastructure</li> <li>Reduced risk of being Phished</li> <li>Blocking user access is via certificate revocation</li> </ul>	<ul style="list-style-type: none"> <li>PKI infrastructure is required</li> <li>Users must configure supplicant to use certificate*</li> <li>Identity may be exposed in TLS exchange depending on contents of certificate</li> </ul>
EAP-TTLS	Mac OS X, Linux, iOS (iPhone, iPod Touch, iPad), Android (v1.6+)		<ul style="list-style-type: none"> <li>No native supplicant support on Microsoft Windows</li> <li>Potential for Man-in-the-Middle attacks*</li> </ul>
EAP-PEAP	Windows (XP, Vista, 7), Mac OS X, Linux, iOS (iPhone, iPod Touch, iPad), Android (v1.6+)	<ul style="list-style-type: none"> <li>Works on many platforms</li> </ul>	<ul style="list-style-type: none"> <li>Potential for Man-in-the-Middle attacks*</li> <li>Identity may be exposed during Phase 1 of exchange</li> </ul>

# Inner Tunnel

IAS  
Institute for Advanced Study

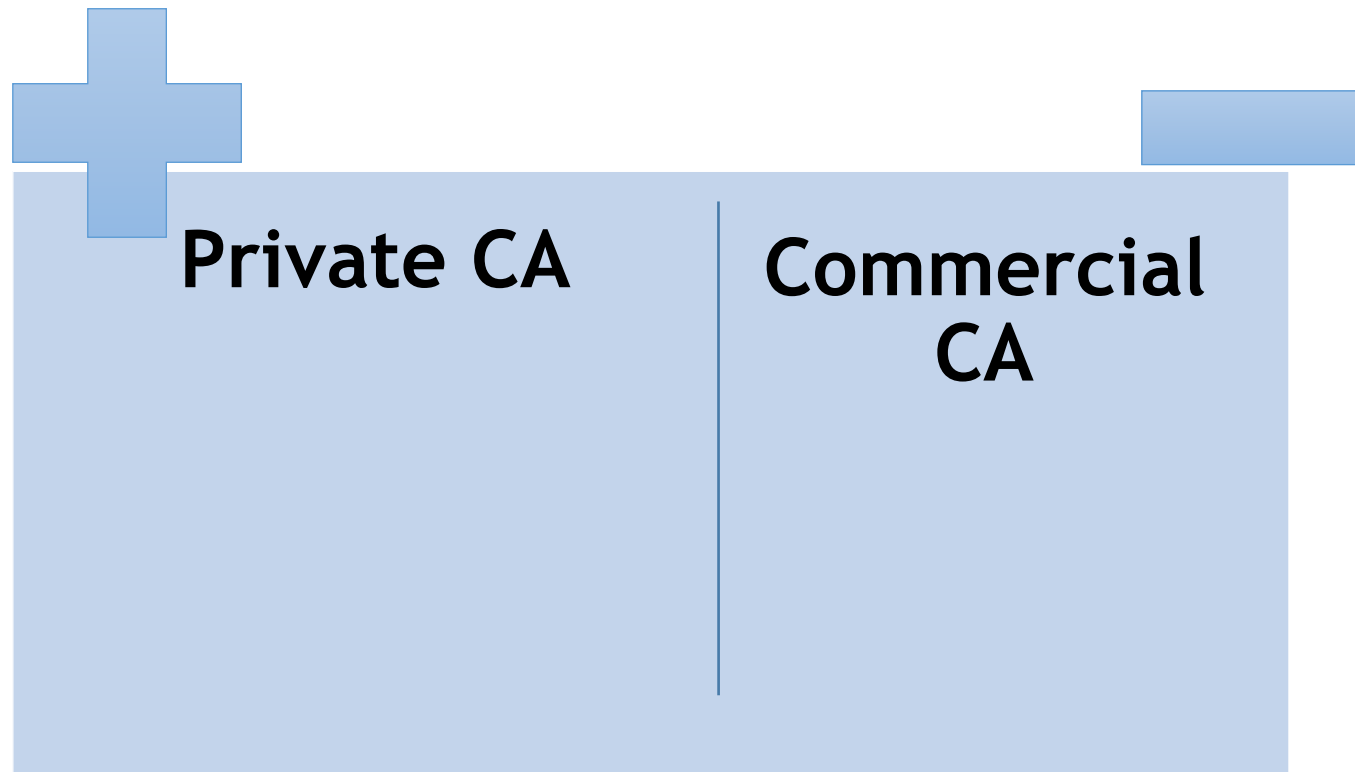
CHAP

MSCHAP

MSCHAPv  
2

PAP

RFC5281 states that "When either client or server receives a certificate as part of the TLS handshake, it should validate the certification path to a trusted root."



# fticks

Audit  
Logging

# Nagios

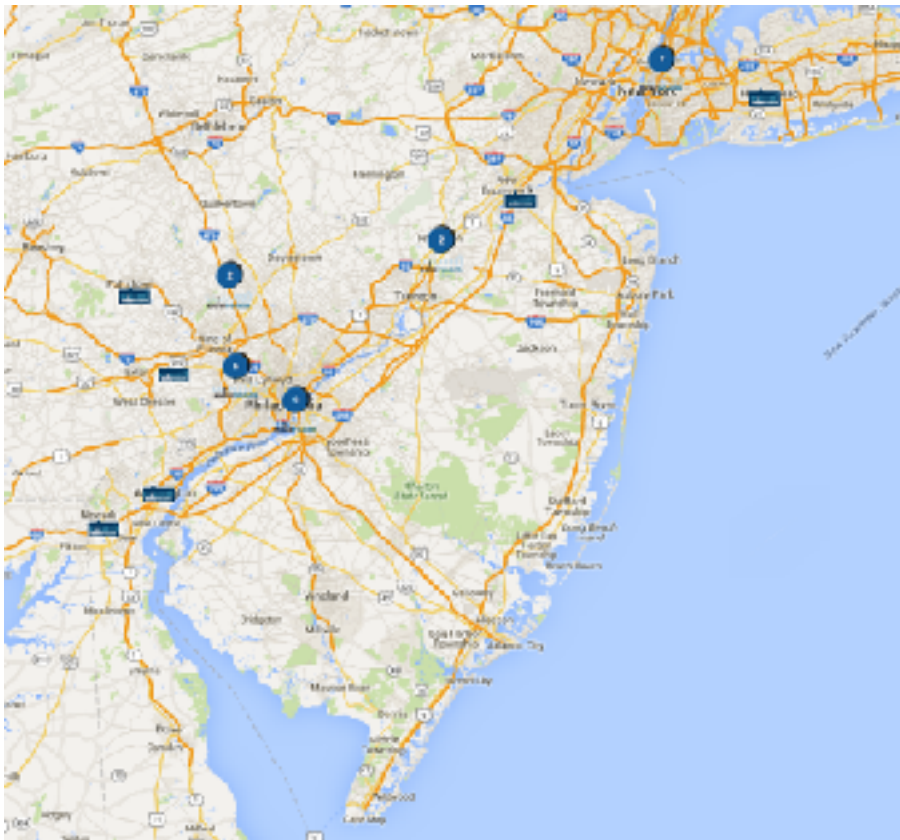
# External

Monitoring

eduroam @  
conference.njedge.net/2015/



<https://www.youtube.com/watch?v=TVCmcMZS3uA&feature=youtu.be>



eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions by simply opening their laptop.

what is eduroam? Generic version

