eduroam

Geert Jan de Groot
based on slides by Paul Dekkers - SURFnet

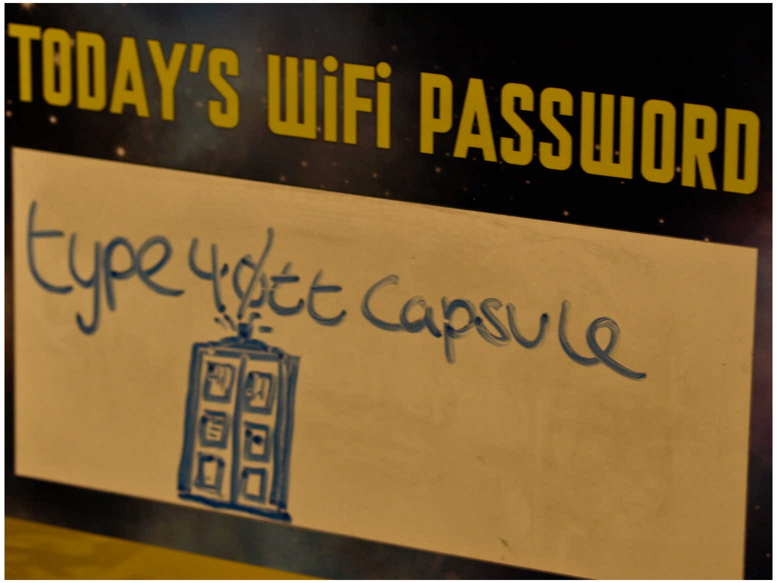
Universities do..

Universities and research institutions do

- Teach
- Research
- Co-operate

Co-operation

- To work together, you must communicate
  - Visit each other
  - People exchanges?
- Accessing a network is hard
  - Local network or remote
  - One wifi password just does not scale
  - You want individual passwords
    - accountability, people leaving, …
- Login portals suck
  - Typing in passwords is cumbersome
  - Over and over
  - And how about mobile phone w/ wifi? Small keyboards? yuk!



- Wi-fi access methods
  - Open access (no password)
  - Open access with portal
  - WEP
  - WPA/WPA2 with PSK (Private Shared Key)
  - WPA/WPA2 with 802.1X (“WPA enterprise”)

WPA enterprise

- WPA enterprise uses 802.1x technologies
  - “authenticate using username and password” - individual!
  - Authenticate using RADIUS (which SSE did yesterday!)
  - Login is automatic, like with others
    - Open laptop, network!
    - But, it’s authenticated

```
steve    Cleartext-Password := “AfricaWorldCup!”
bob      Cleartext-Password := "s3cr3t"
john     Cleartext-Password := "ilovejane"
jane     Cleartext-Password := "ilovejohn"
```

Guests from other networks

- Guest accounts are a pain
  - Administration, synchronisation

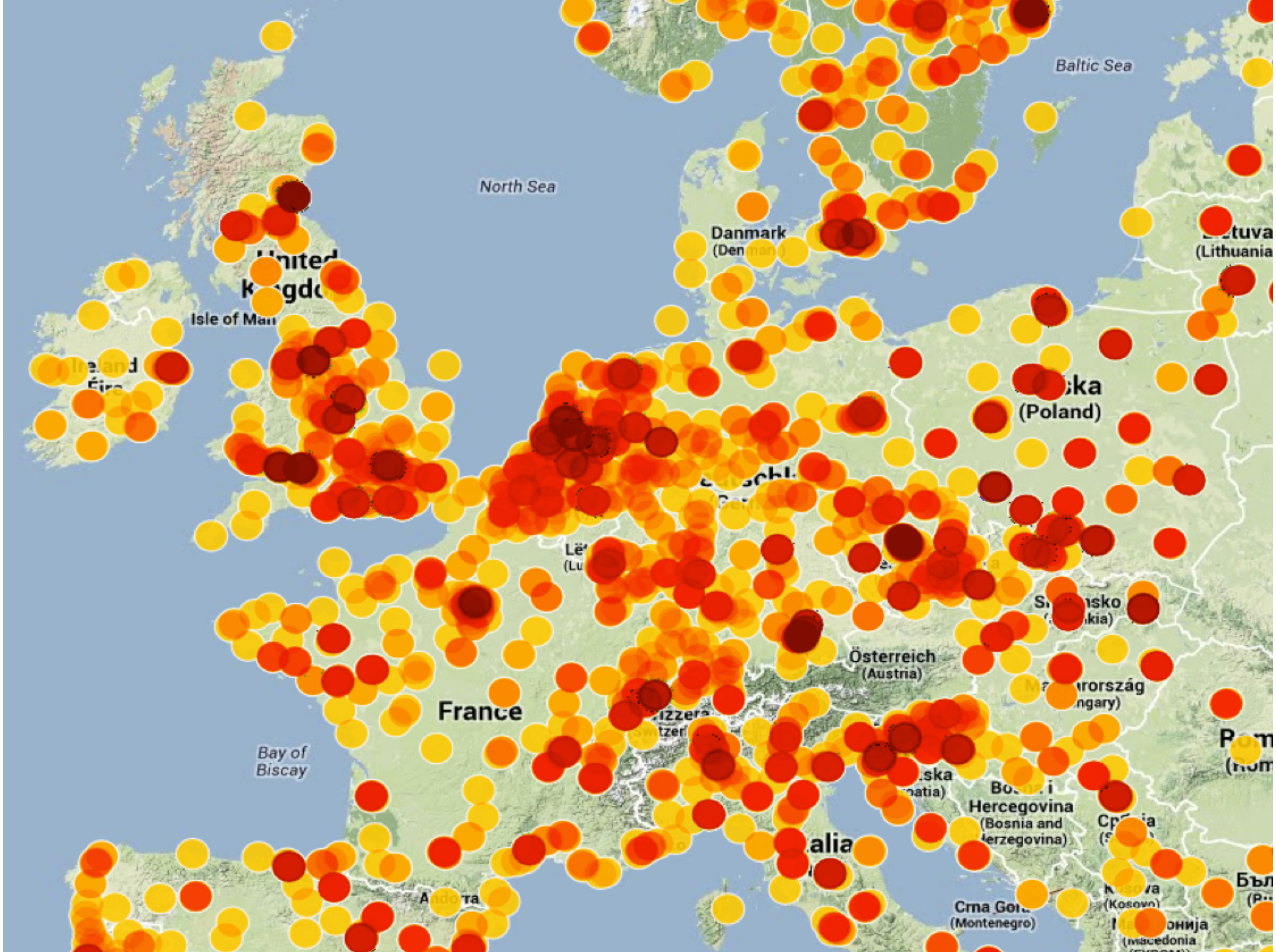
- RADIUS allows confederations
  - joe@blue-university.sd
  - jane@green-university.ng

- RADIUS confederations allow referrals to other RADIUS servers
  - joe@blue-university.sd -> RADIUS at blue-university.sd
  - jane@green-university.ng -> RADIUS at green-university.ng
- No local administration of guest accounts!

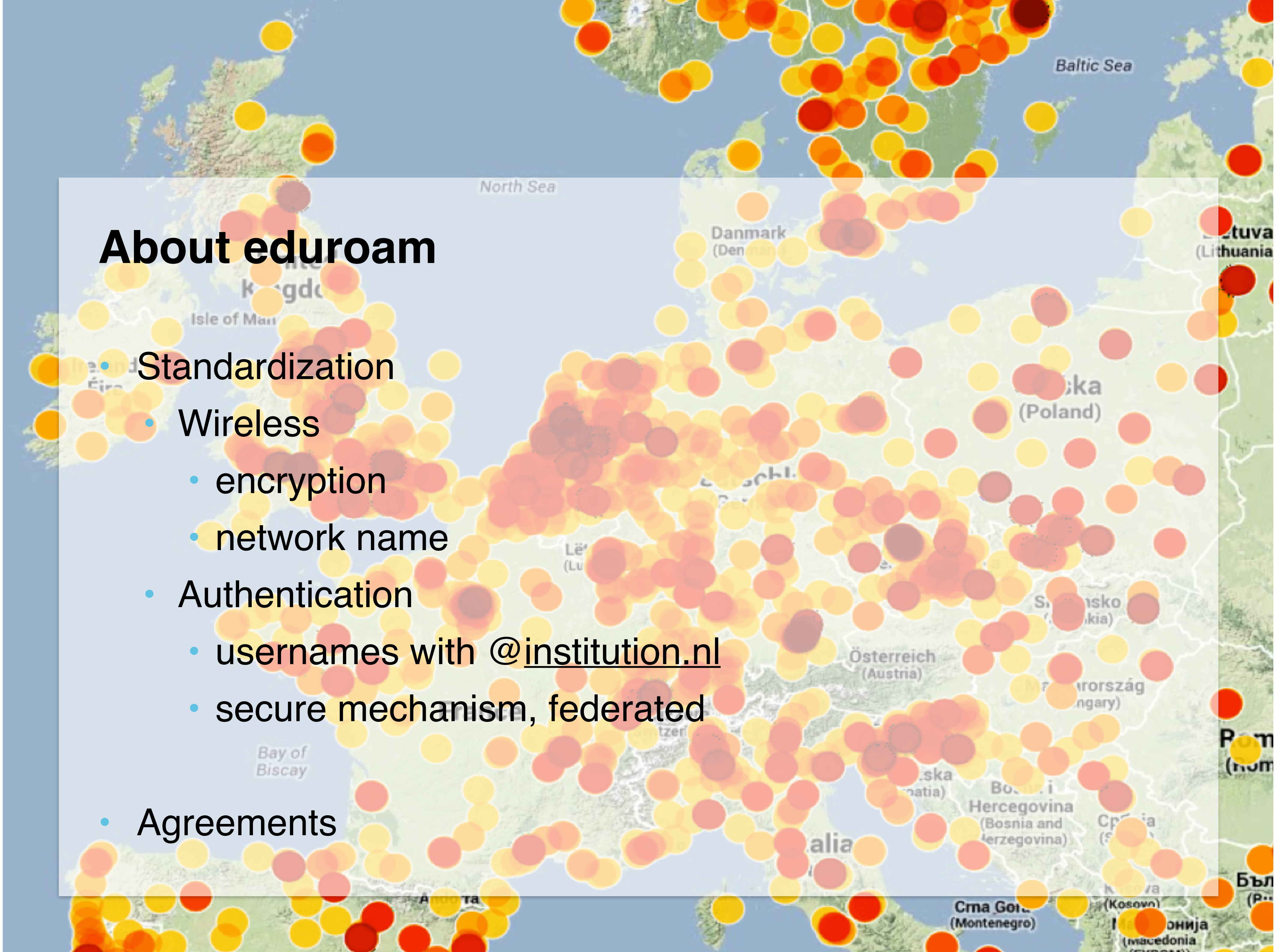
Putting it together

- The Wifi network ‘eduroam’ uses WPA enterprise, RADIUS confederations
- When joe@blue-university.sd visits your institution he connects to the ‘eduroam’ network.
- User gets authenticated using his home RADIUS-server
  - Authenticated access
  - Fully automatic - open up laptop, connected
- You accept my guests, I accept your guests

- Doing eduroam at AfNOG for awareness, testing, play and fun!

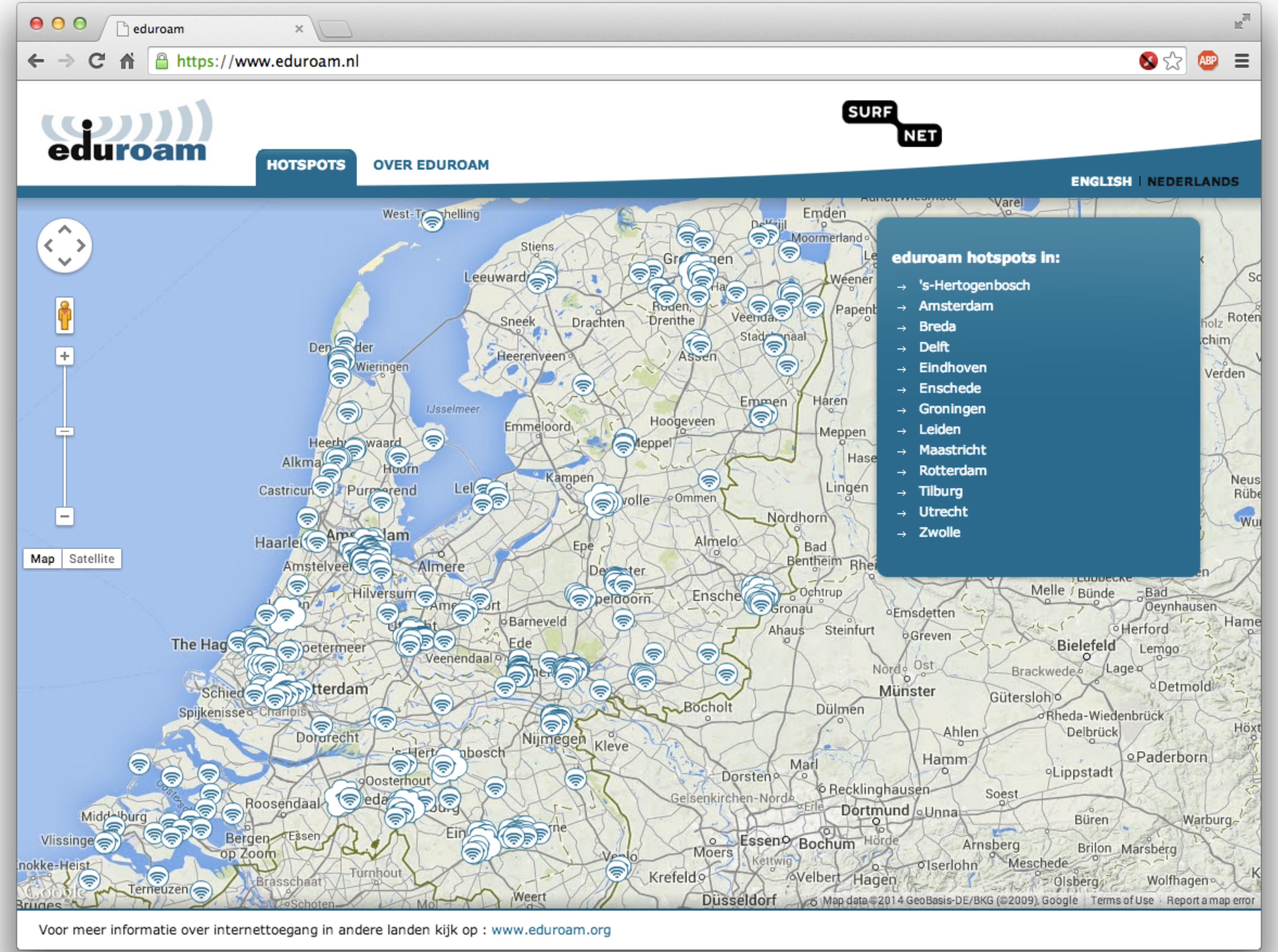


Baltic Sea
North Sea
Danmark
(Denmark)
United Kingdom
Isle of Man
Ireland
Éire
Lietuva
(Lithuania)
Polska
(Poland)
Deutschland
(Germany)
Lëtzebuerg
(Luxembourg)
Slovensko
(Slovakia)
Österreich
(Austria)
Magyarország
(Hungary)
France
Schweiz
Svizzera
Bay of
Biscay
Hrvatska
(Croatia)
Bosna i
Hercegovina
(Bosnia and
Herzegovina)
Србија
(Serbia)
Italia
Andorra
Crna Gora
(Montenegro)
Kosova
(Kosovo)
Македонија
(Macedonia
Бъл
Rom
(Rom



About eduroam

- Standardization
    - Wireless
        - encryption
        - network name
    - Authentication
        - usernames with @institution.nl
        - secure mechanism, federated
- Agreements



eduroam hotspots in:

→ 's-Hertogenbosch
→ Amsterdam
→ Breda
→ Delft
→ Eindhoven
→ Enschede
→ Groningen
→ Leiden
→ Maastricht
→ Rotterdam
→ Tilburg
→ Utrecht
→ Zwolle

Map data ©2014 GeoBasis-DE/BKG (©2009), Google Terms of Use Report a map error

Voor meer informatie over internettoegang in andere landen kijk op : www.eduroam.org

Why did we start eduroam

- **Security problems**,
  traditional wireless LAN is not safe:
  - who is (ab)using the (wireless) network?
  - are people eavesdropping?
  - weak (or no) encryption, authentication
- **Difficult to allow guests**
  - User-identification
  - Distribute secrets?
- **Users are mobile**
  (Bologna process, ECTS, …)

Why did we start eduroam

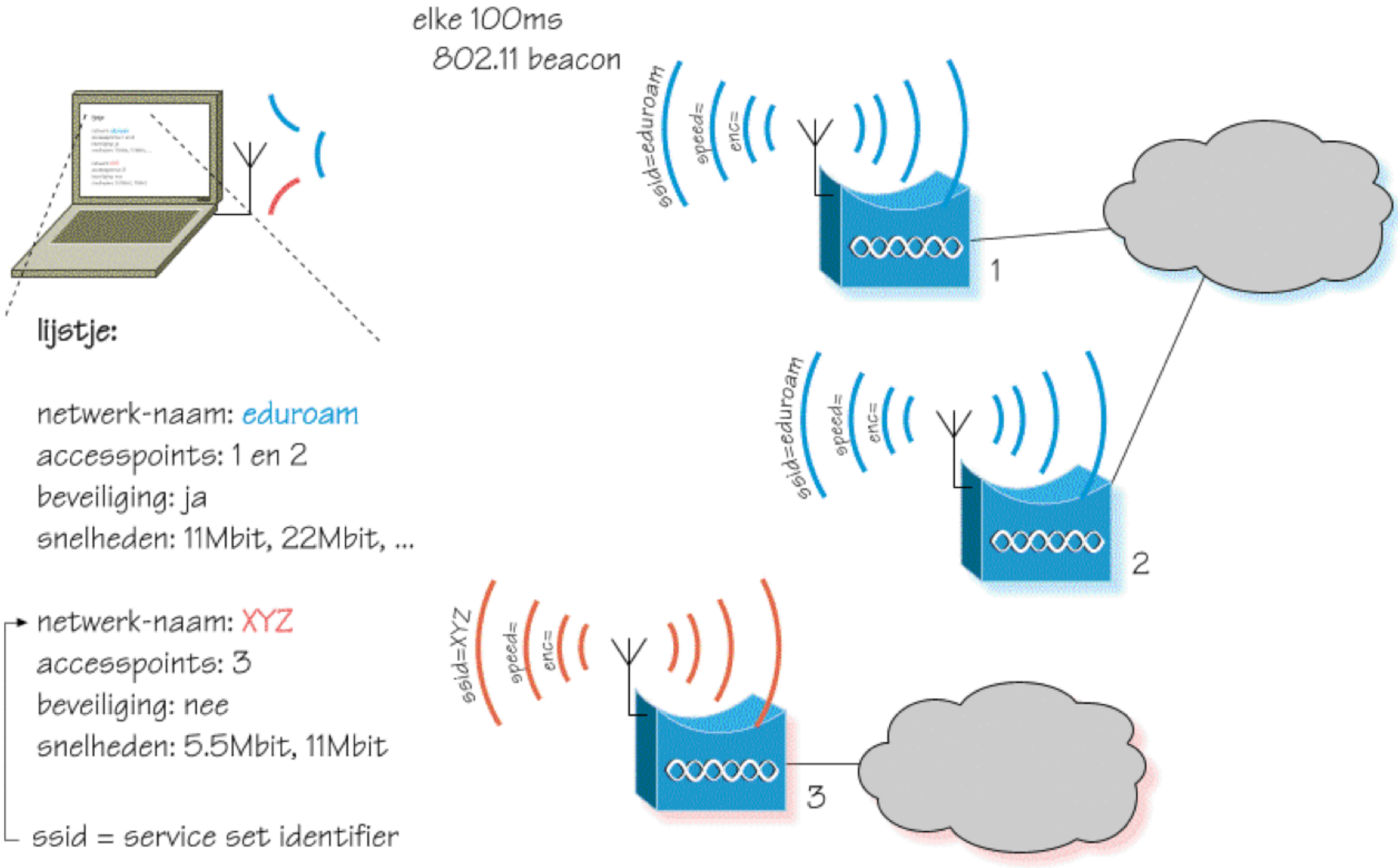
- **Ease of use!**
  Always connected (like 2/3/4G? *))
  Even on busy places, in cities, …

Open up your laptop and bang! You're online

**) mobile data doesn't always work well on crowded locations or in buildings, Wi-Fi / eduroam can be used for seamlessly offloading data*

4G won't replace Wi-Fi, they both have their own roadmap

Wireless



lijstje:

netwerk-naam: eduroam
accesspoints: 1 en 2
beveiliging: ja
snelheden: 11Mbit, 22Mbit, ...

netwerk-naam: XYZ
accesspoints: 3
beveiliging: nee
snelheden: 5.5Mbit, 11Mbit

ssid = service set identifier

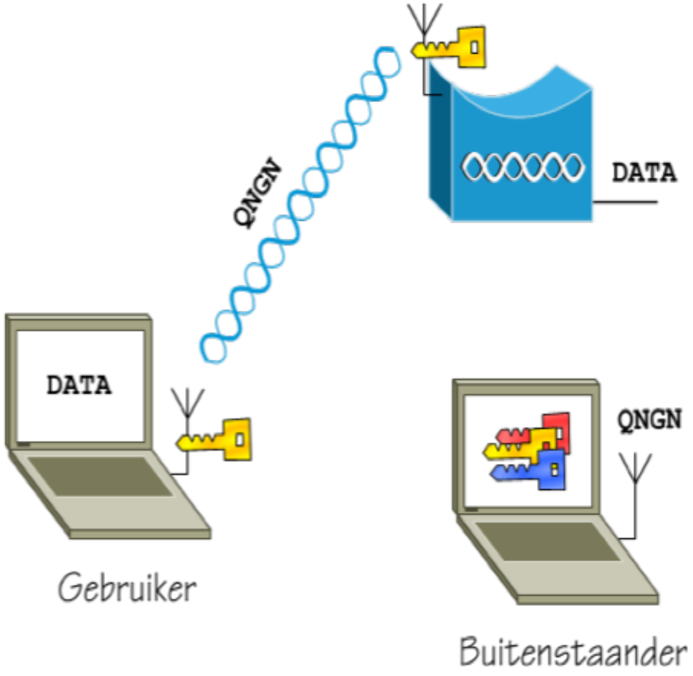
Wireless and basic security

- Every network has a name:
  an (in)visible SSID (Service Set Identifier)

- Possible to restrict on MAC addresses

- Access / encryption with “keys”
  - WEP, Wired Equivalent Privacy
  - WPA(2), with pre-shared key (PSK)

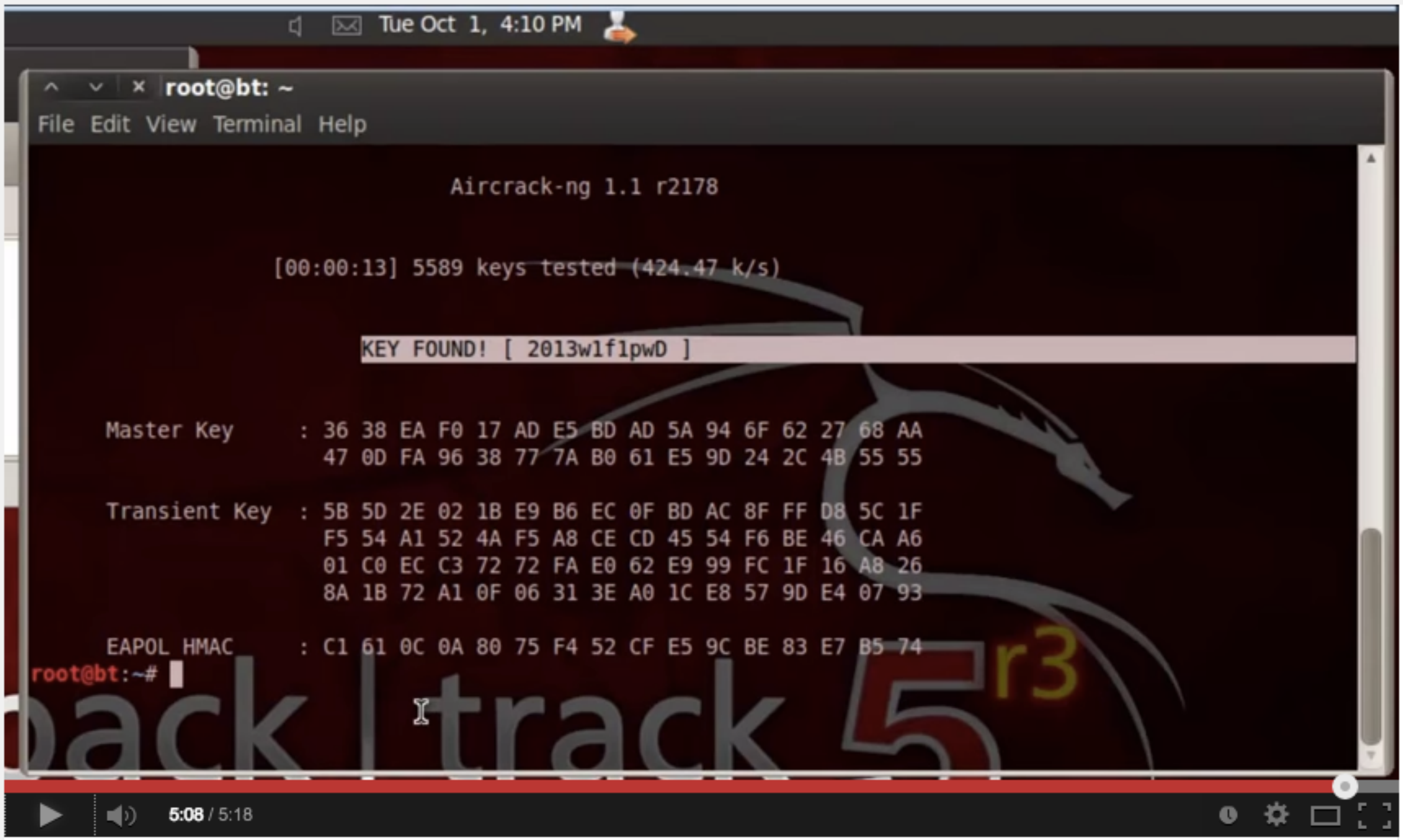
- Wi-Fi Protected Setup (WPS)
  - easier setup, with a PIN
    no need for SSID or key



Sorry: all of this is insecure…

- Invisible SSID?
  - You need the SSID to associate to a (hidden) network, so just wait for someone to associate
  - Without encryption, easy to eaves-drop, spoof / steal a session, inject packages (MitM)
  - MAC security? Easy to spoof!
- WEP uses weak RC4 encryption
- WPA keys can be “recovered” with (re)association
- WPS is required for Wi-Fi certification, but:
  - The PIN can be brute forced

“Computervredebreuk” is too easy
Tools are easy to find! Aircrack-ng, Reaver

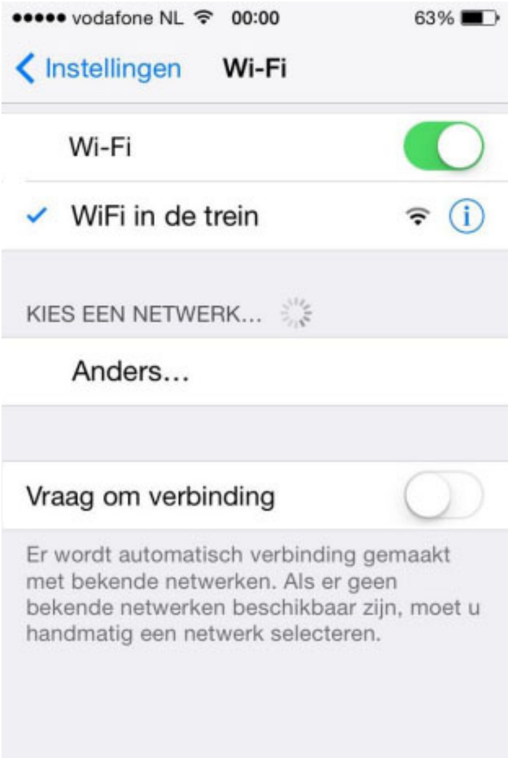


```
                              Aircrack-ng 1.1 r2178


                   [00:00:13] 5589 keys tested (424.47 k/s)


                          KEY FOUND! [ 2013w1f1pwD ]


      Master Key     : 36 38 EA F0 17 AD E5 BD AD 5A 94 6F 62 27 68 AA
                       47 0D FA 96 38 77 7A B0 61 E5 9D 24 2C 4B 55 55

      Transient Key  : 5B 5D 2E 02 1B E9 B6 EC 0F BD AC 8F FF D8 5C 1F
                       F5 54 A1 52 4A F5 A8 CE CD 45 54 F6 BE 46 CA A6
                       01 C0 EC C3 72 72 FA E0 62 E9 99 FC 1F 16 A8 26
                       8A 1B 72 A1 0F 06 31 3E A0 1C E8 57 9D E4 07 93

      EAPOL HMAC     : C1 61 0C 0A 80 75 F4 52 CF E5 9C BE 83 E7 B5 74
root@bt:~#
```

Cracking Wpa & Wpa2 in 5 mins using BackTrack 5 R3

Open wireless network

- … was always a bad idea:
  - who is (ab)using the network?
  - are people eavesdropping?
- Weak encryption, no authentication, no traceability
- Perfect Man-in-the-Middle
  - easy to make a rogue Access Point
  - required VPN or end-to-end encryption
  - OpenSSL vulnerabilities and unpatched devices (Android!) are more risky than ever before



●●●●● vodafone NL 00:00 63%

Instellingen Wi-Fi

Wi-Fi

✓ WiFi in de trein

KIES EEN NETWERK...

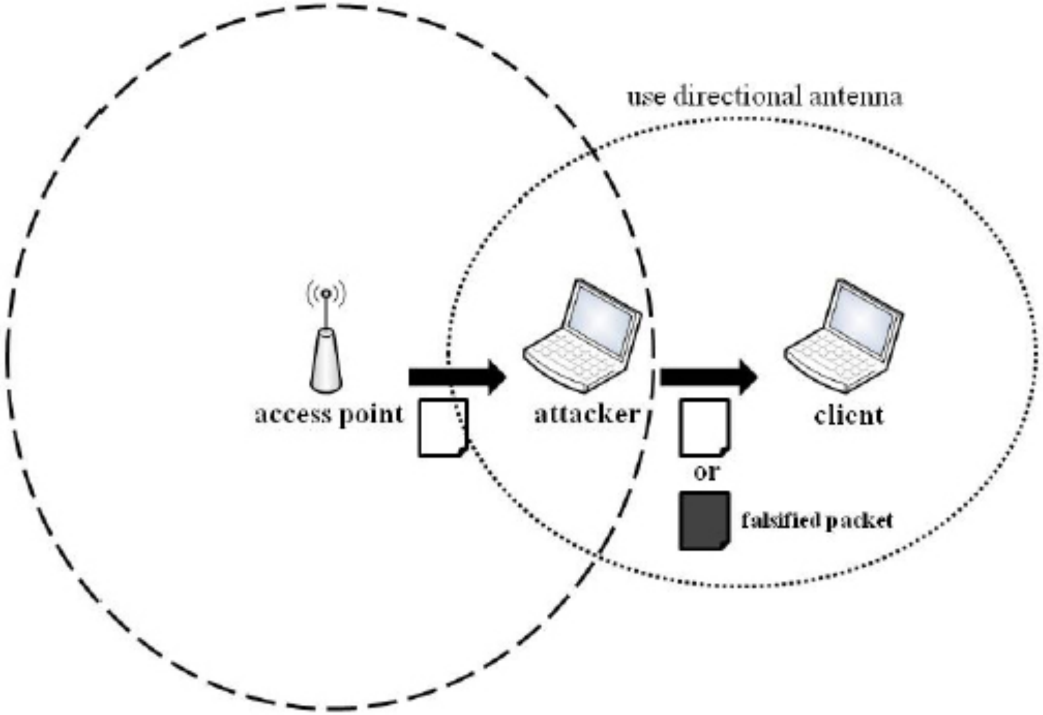
Anders...

Vraag om verbinding

Er wordt automatisch verbinding gemaakt met bekende netwerken. Als er geen bekende netwerken beschikbaar zijn, moet u handmatig een netwerk selecteren.

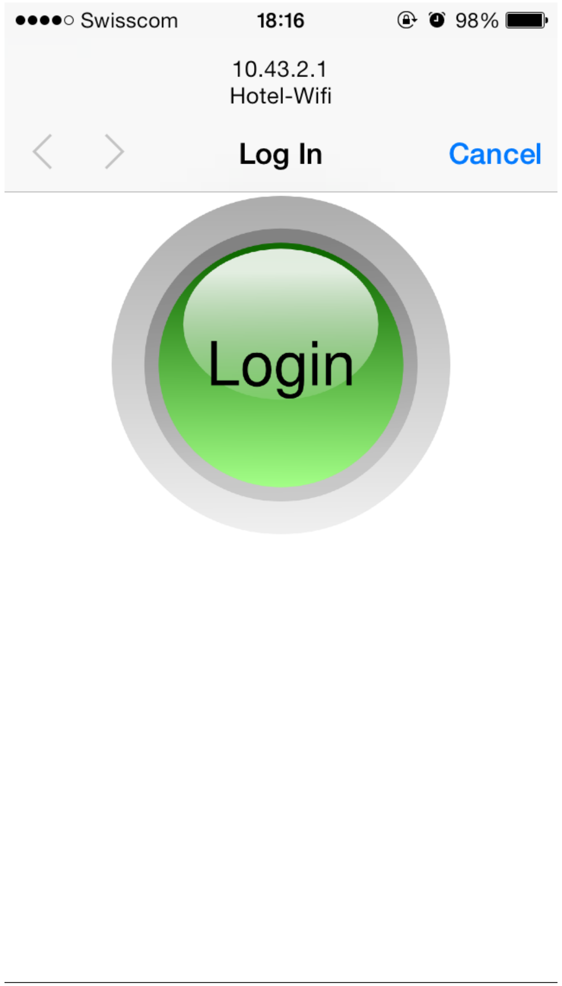
OpenSSL vulnerabilities (Android oops)

- SSL is everywhere
- CVE-2014-0224 and SSLv3 vulnerability made this worse



Open wireless with captive portal

- **Captive portals are insecure**
  - Not possible to check **certificate revocation**
  - **OCSP** (online service) is unreachable (or can be made so, with soft-fail)
  - Still easy to create a **Man-in-the-Middle**



- Easy to create a **Rogue AP**
  - Tethering on your phone, can even call this “t-mobile” or “KPN”…

So we needed something better

- Ease of use:

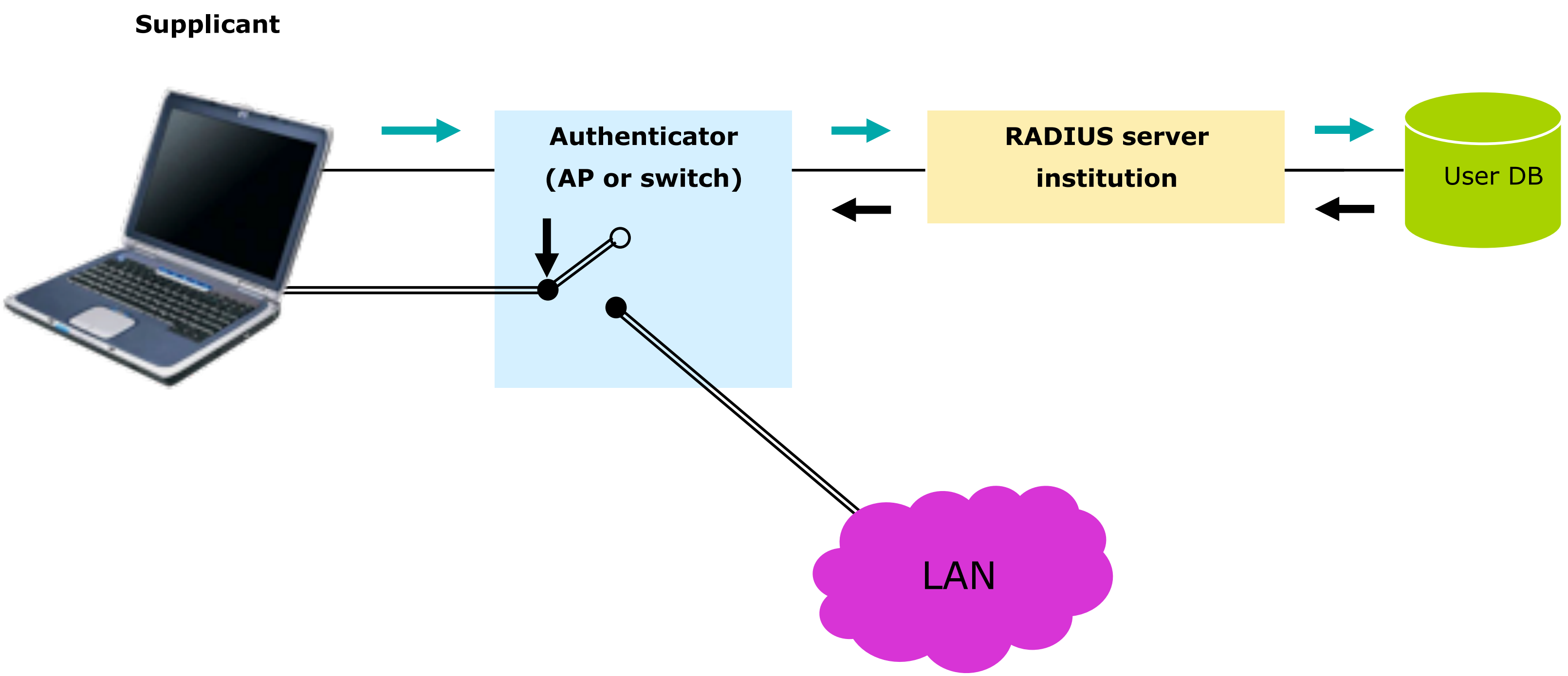
  Open up your laptop and bang! You’re online!
- Identify users at the edge of the network
- Scalable: use existing user administration
- Open standards,

  future proof
- Secure
- Allow guests

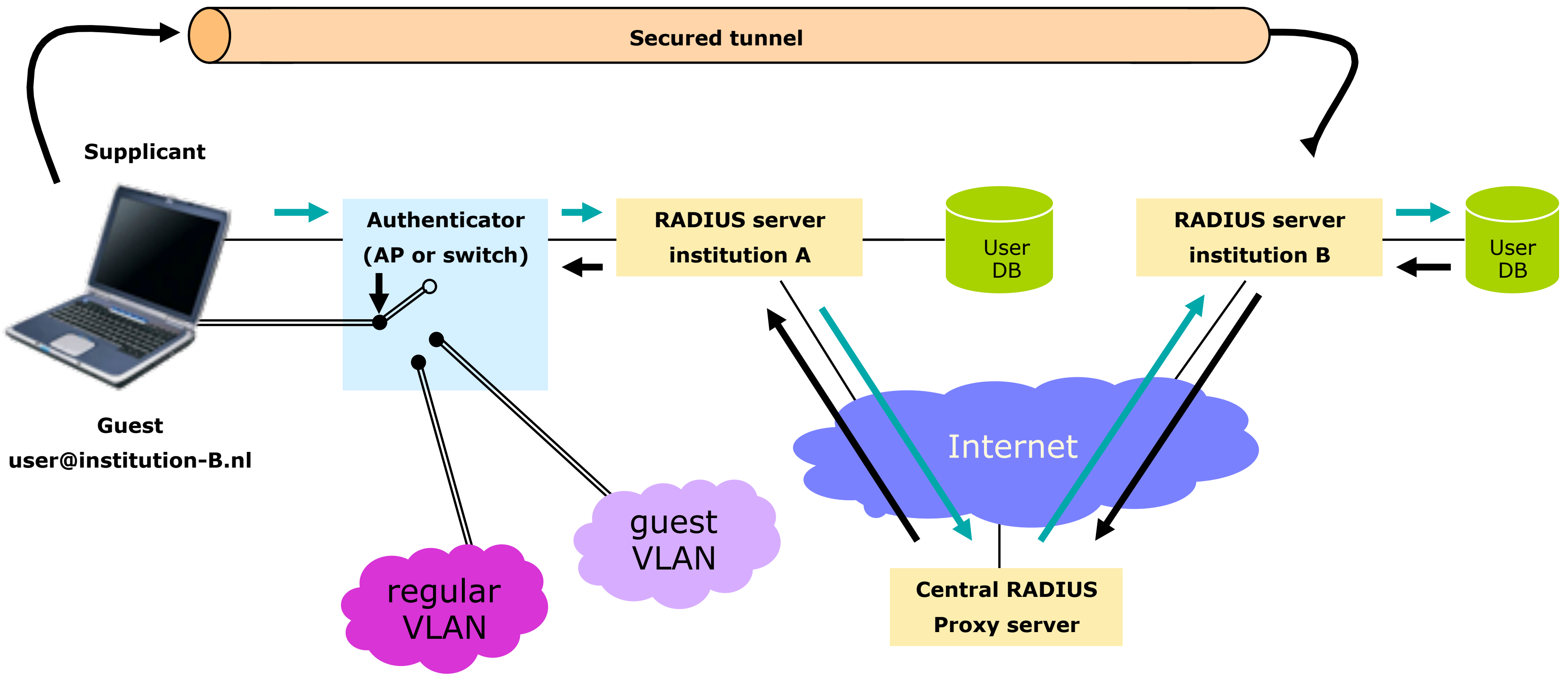
- Set a standard:

802.1x

- “Port” based authentication



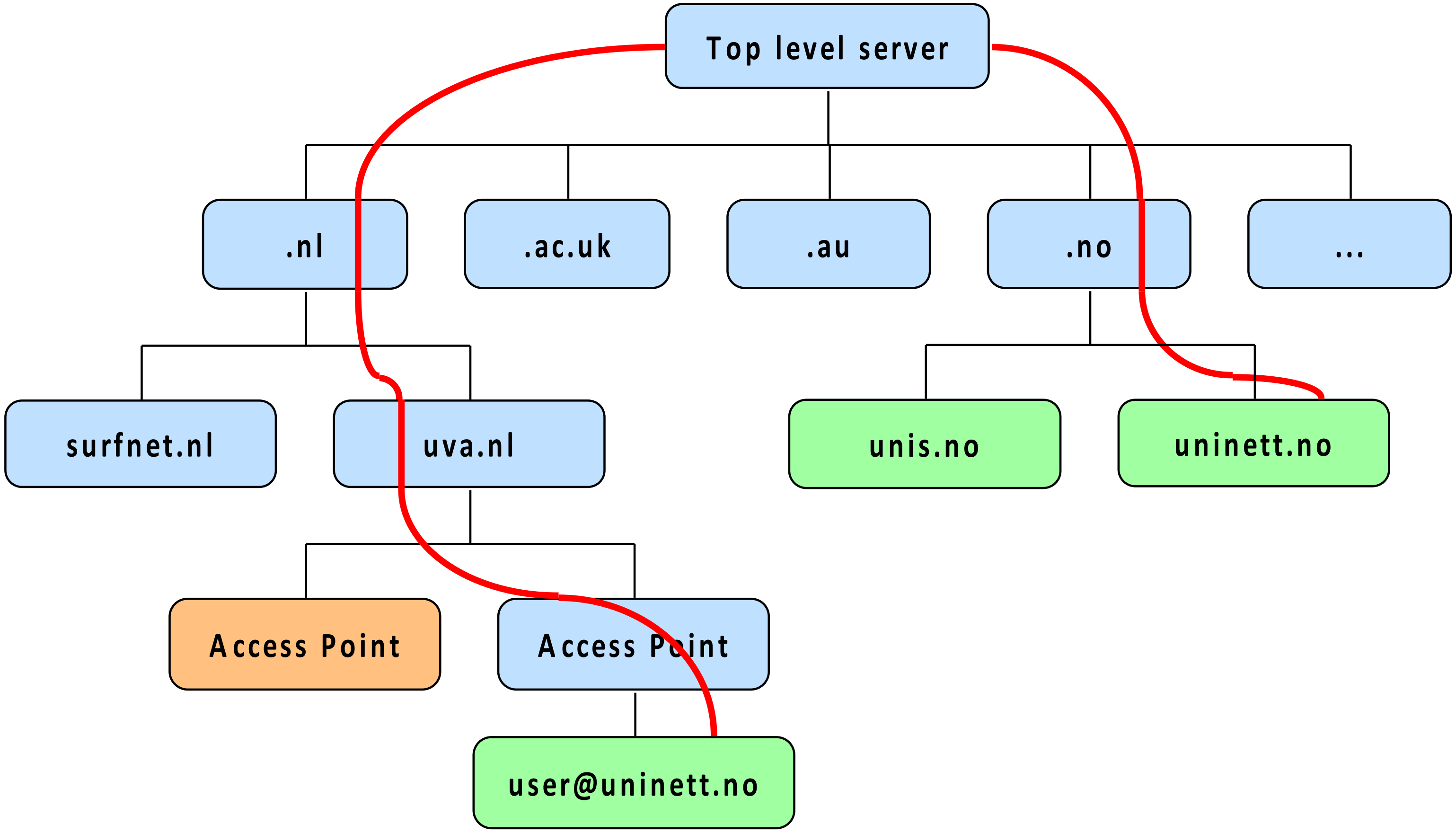
802.1x and guest usage: eduroam!



802.1x and EAP

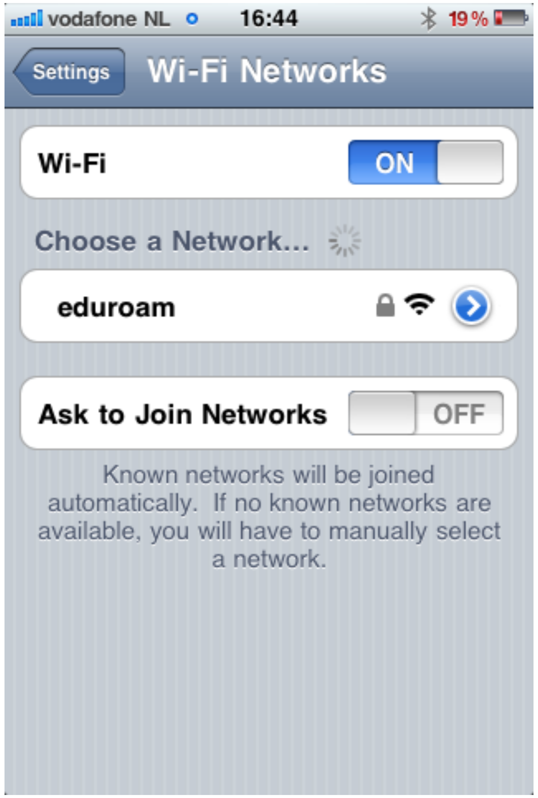
- Extensible Authentication Protocol
- Different EAP-types
- The (home-)organization decides type for their users
- EAP-types with SSL/TLS
  - “Mutual authentication”
  - Encryption keys are derived from SSL session
- EAP is transported and proxied in RADIUS

Secure international roaming



Client configuration eduroam

- 3 step configuration
- IdP pinning



Wi-Fi Networks

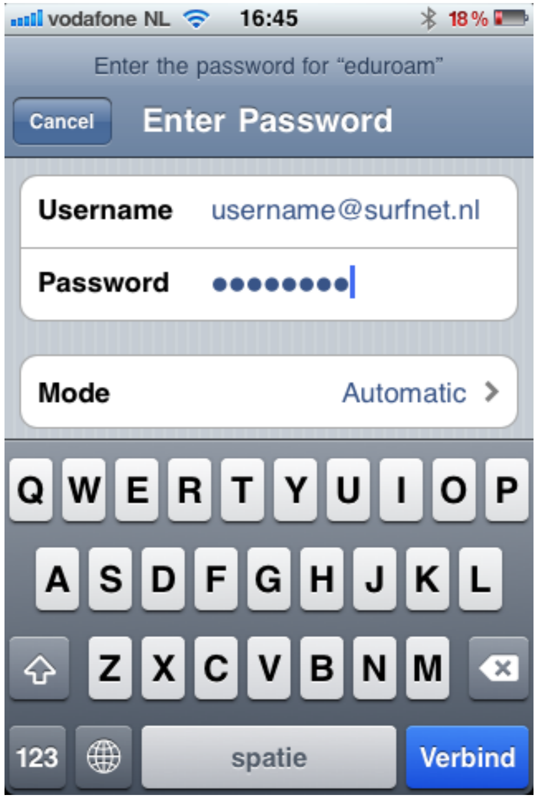
Wi-Fi ON

Choose a Network...

eduroam

Ask to Join Networks OFF

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.



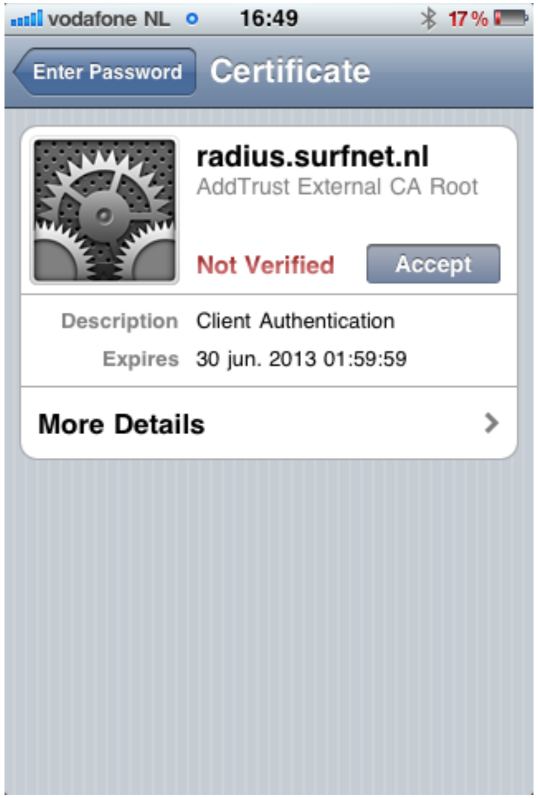
Enter the password for "eduroam"

Enter Password

Username username@surfnet.nl

Password ●●●●●●●●●

Mode Automatic



Certificate

radius.surfnet.nl

AddTrust External CA Root

Not Verified

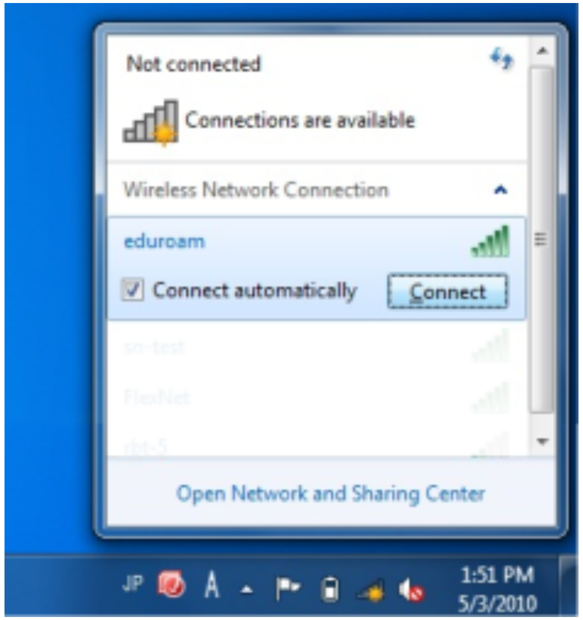
Description Client Authentication

Expires 30 jun. 2013 01:59:59

More Details

Client configuration eduroam

- Windows just as easy: 3 steps



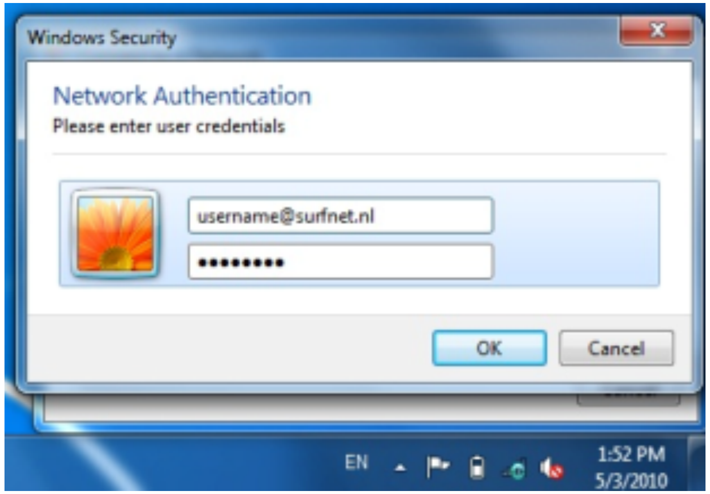
Not connected

Connections are available

Wireless Network Connection

eduroam

☑ Connect automatically



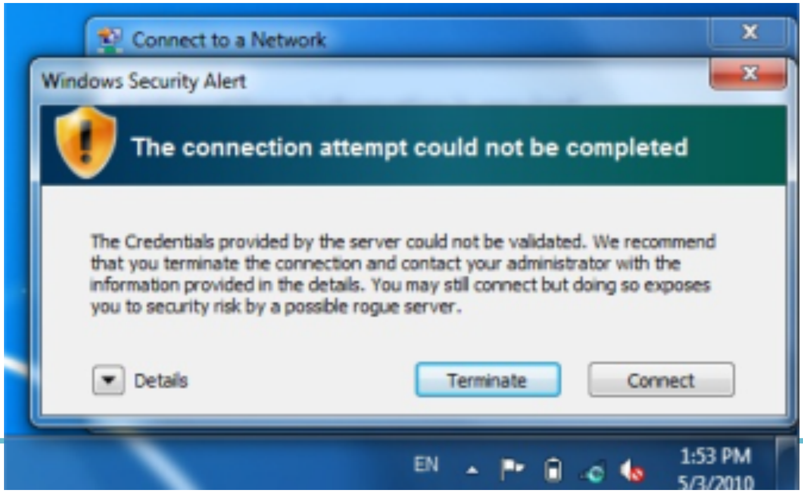
Windows Security

Network Authentication

Please enter user credentials

username@surfnet.nl

•••••••••



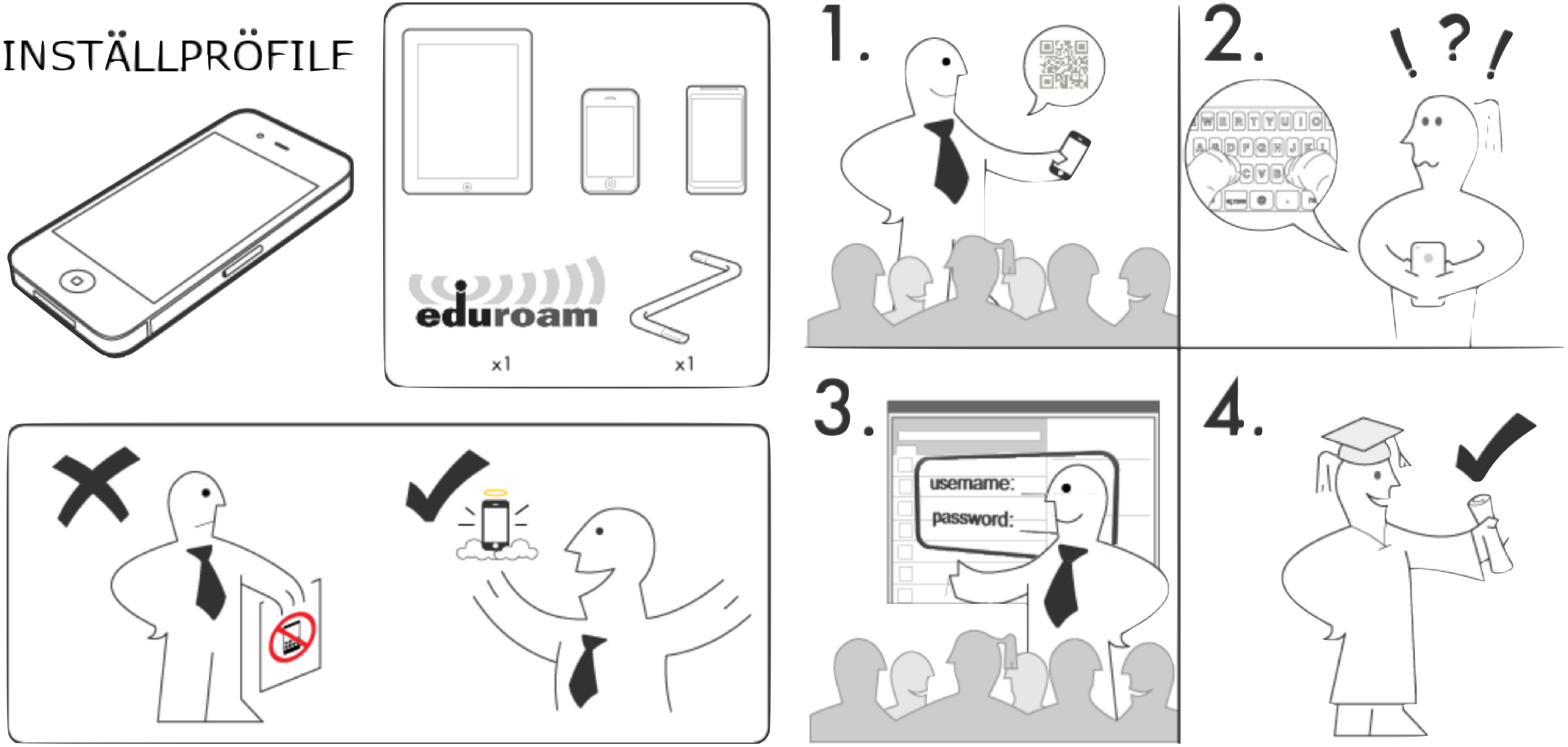
Connect to a Network

Windows Security Alert

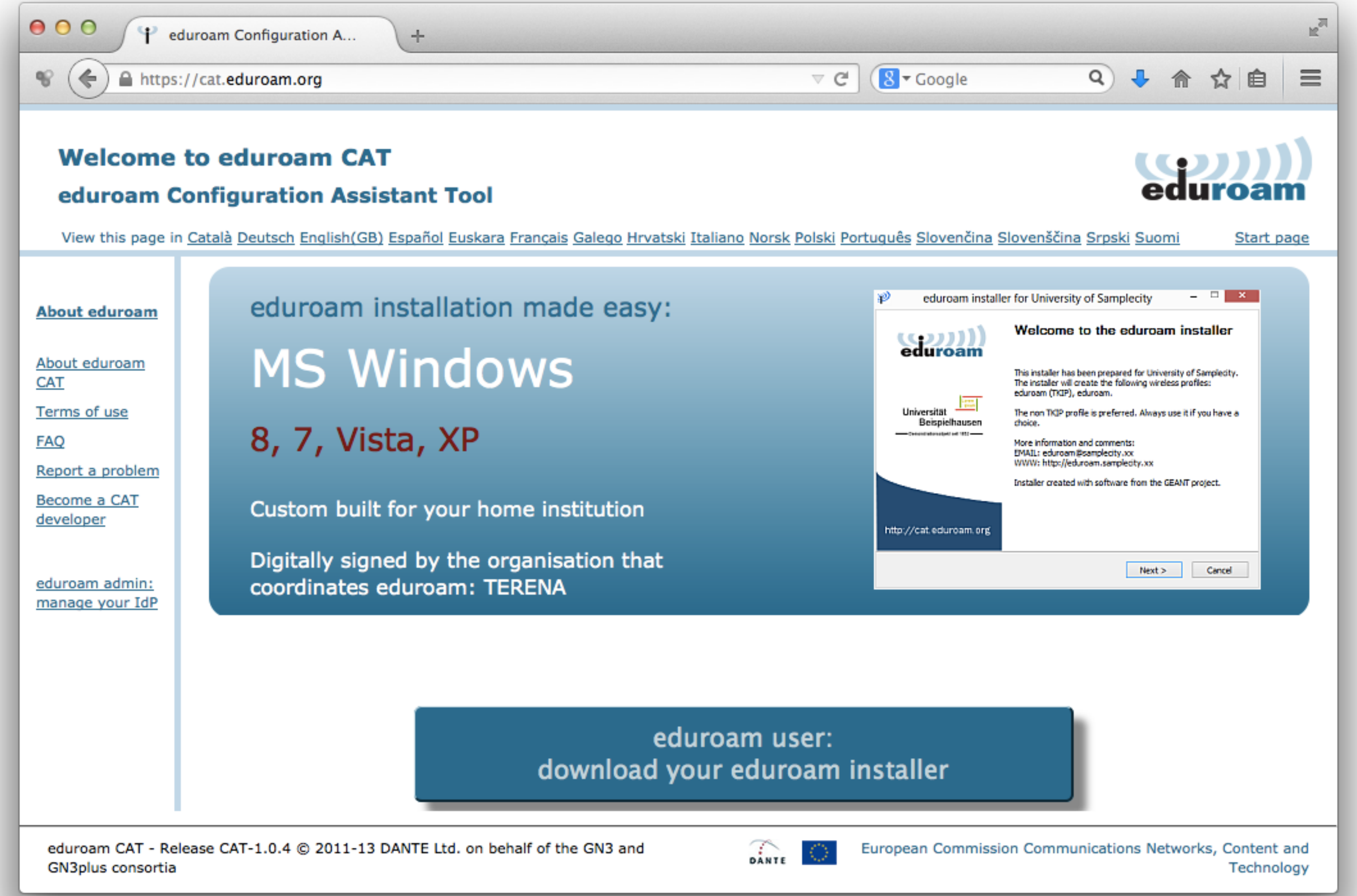
The connection attempt could not be completed

The Credentials provided by the server could not be validated. We recommend that you terminate the connection and contact your administrator with the information provided in the details. You may still connect but doing so exposes you to security risk by a possible rogue server.

Client configuration eduroam



eduroam CAT



Welcome to eduroam CAT

eduroam Configuration Assistant Tool

View this page in Català Deutsch English(GB) Español Euskara Français Galego Hrvatski Italiano Norsk Polski Português Slovenčina Slovenščina Srpski Suomi

Start page

About eduroam

About eduroam CAT

Terms of use

FAQ

Report a problem

Become a CAT developer

eduroam admin: manage your IdP

eduroam installation made easy:

MS Windows

8, 7, Vista, XP

Custom built for your home institution

Digitally signed by the organisation that coordinates eduroam: TERENA

eduroam installer for University of Samplecity

Welcome to the eduroam installer

This installer has been prepared for University of Samplecity.
The installer will create the following wireless profiles:
eduroam (TKIP), eduroam.

The non TKIP profile is preferred. Always use it if you have a choice.

More information and comments:
EMAIL: eduroam@samplecity.xx
WWW: http://eduroam.samplecity.xx

Installer created with software from the GEANT project.

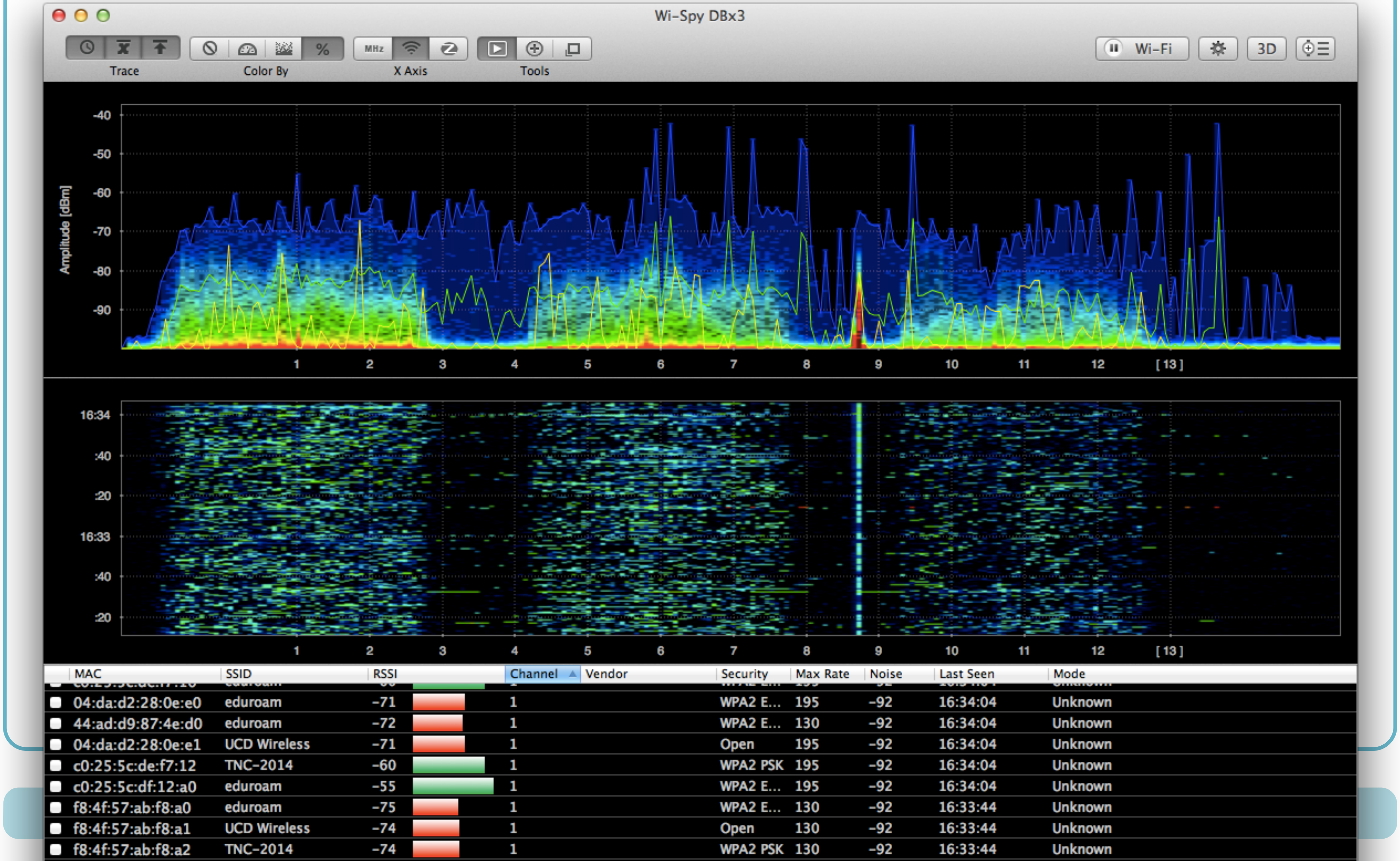
eduroam user:
download your eduroam installer

eduroam CAT - Release CAT-1.0.4 © 2011-13 DANTE Ltd. on behalf of the GN3 and GN3plus consortia

European Commission Communications Networks, Content and Technology

eduroam
YOU HAVE
JUST BEEN
EDUROAMED
YOU HAVE
JUST BEEN
EDUROAMED

Wireless: the RF challenge



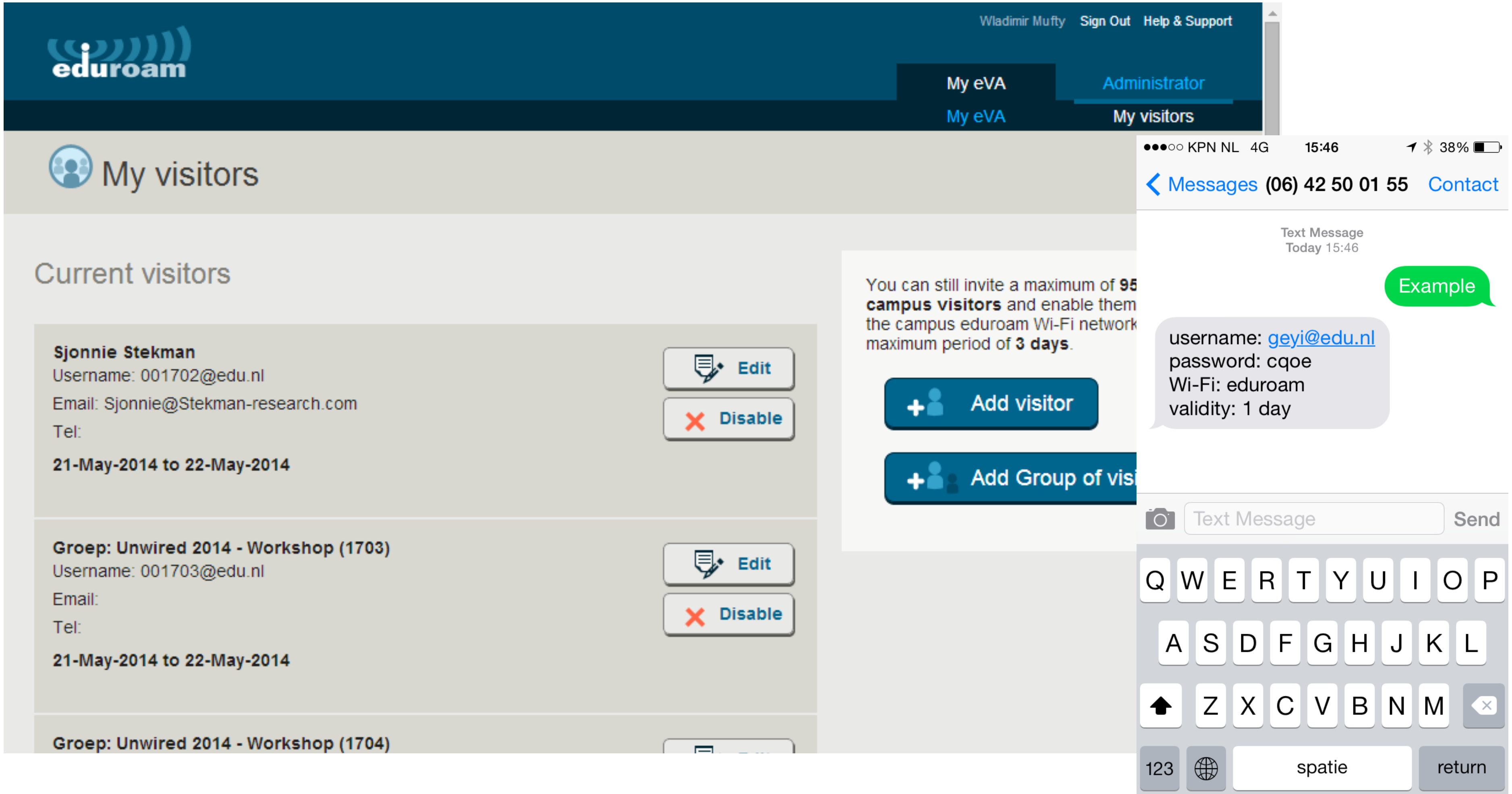
	MAC	SSID	RSSI		Channel ▲	Vendor	Security	Max Rate	Noise	Last Seen	Mode
□	04:da:d2:28:0e:e0	eduroam	-71	🟥	1		WPA2 E...	195	-92	16:34:04	Unknown
□	44:ad:d9:87:4e:d0	eduroam	-72	🟥	1		WPA2 E...	130	-92	16:34:04	Unknown
□	04:da:d2:28:0e:e1	UCD Wireless	-71	🟥	1		Open	195	-92	16:34:04	Unknown
□	c0:25:5c:de:f7:12	TNC-2014	-60	🟩	1		WPA2 PSK	195	-92	16:34:04	Unknown
□	c0:25:5c:df:12:a0	eduroam	-55	🟩	1		WPA2 E...	195	-92	16:34:04	Unknown
□	f8:4f:57:ab:f8:a0	eduroam	-75	🟥	1		WPA2 E...	130	-92	16:33:44	Unknown
□	f8:4f:57:ab:f8:a1	UCD Wireless	-74	🟥	1		Open	130	-92	16:33:44	Unknown
□	f8:4f:57:ab:f8:a2	TNC-2014	-74	🟥	1		WPA2 PSK	130	-92	16:33:44	Unknown

Wireless experience

- A bad Wi-Fi experience, translates to:
  - Frustrated and complaining users
  - “eduroam sucks”
    … even when eduroam is not at fault

- Some planning… makes sense
  - Eg. consider high-density rooms for lectures
    (hotspots vs. overall coverage)
  - Think about the building, AP placement

eduroam Visitor Access (eVA)



My visitors

Current visitors

Sjonnie Stekman
Username: 001702@edu.nl
Email: Sjonnie@Stekman-research.com
Tel:
21-May-2014 to 22-May-2014

Groep: Unwired 2014 - Workshop (1703)
Username: 001703@edu.nl
Email:
Tel:
21-May-2014 to 22-May-2014

Groep: Unwired 2014 - Workshop (1704)

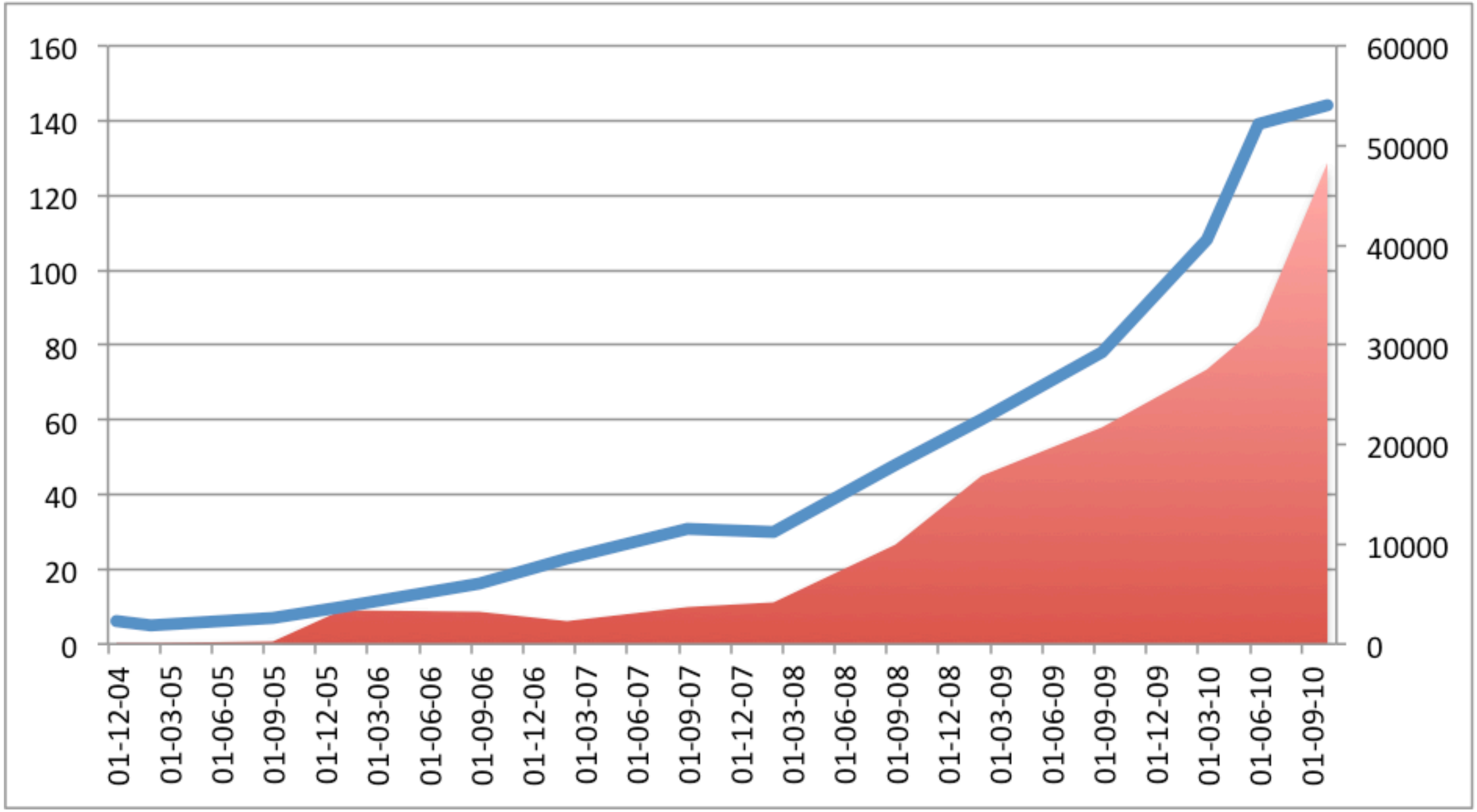
You can still invite a maximum of **95** **campus visitors** and enable them the campus eduroam Wi-Fi network maximum period of **3 days**.

Text Message
Today 15:46

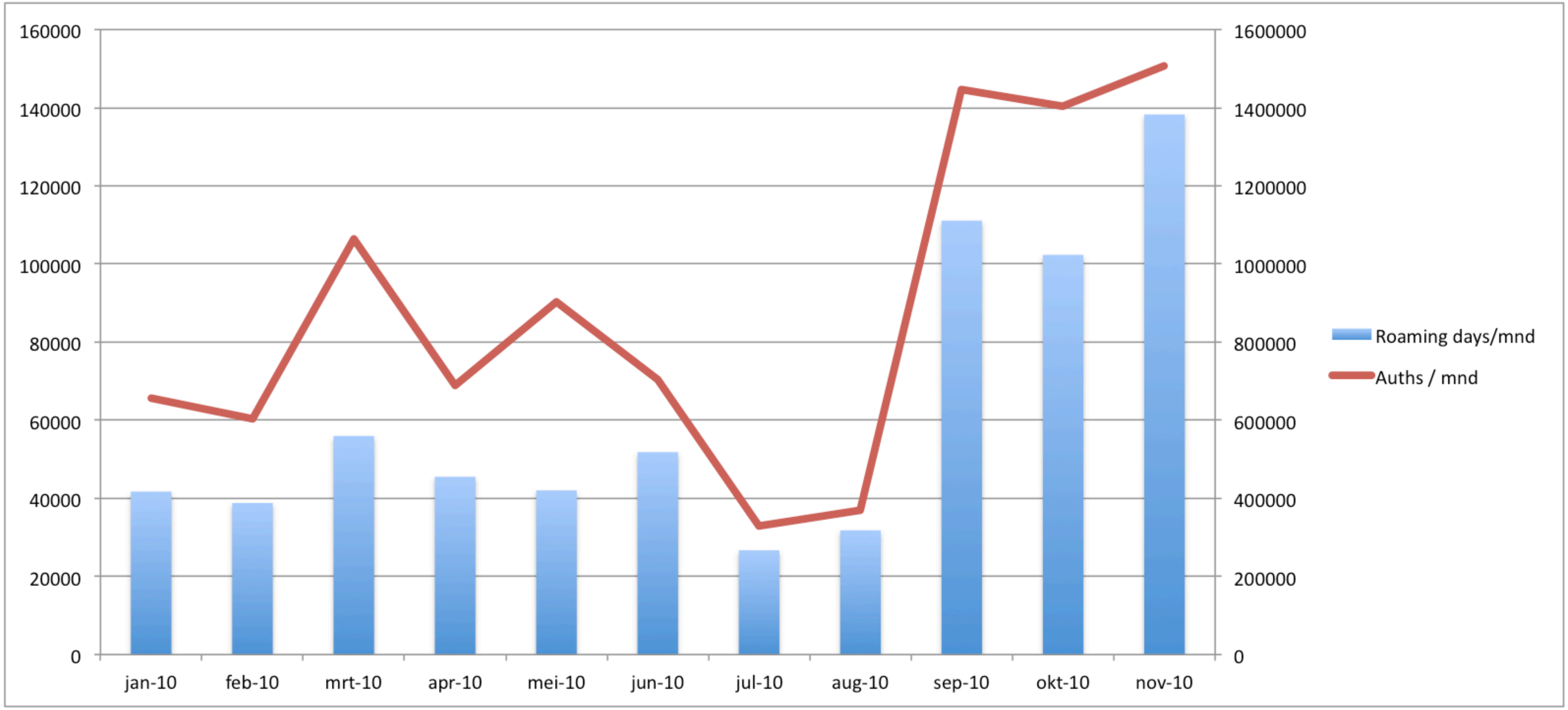
Example

username: geyi@edu.nl
password: cqoe
Wi-Fi: eduroam
validity: 1 day

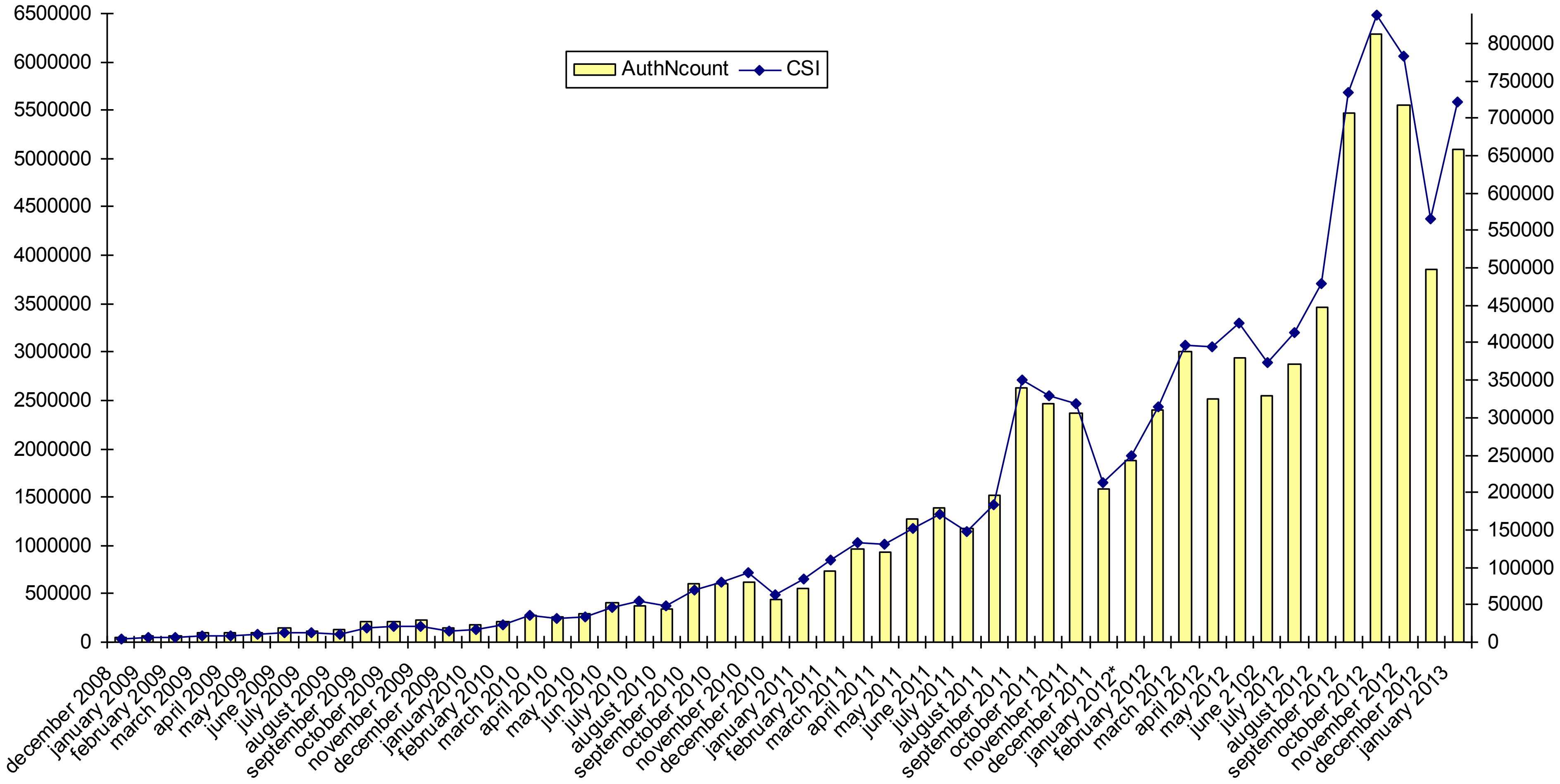
eduroam growth



usage: peak every new semester



Statistics; usage between countries



eduroam in a nutshell (1)

- Wireless
  - SSID eduroam
  - WPA2-Enterprise
- RADIUS
  - authentication in @domain.nl
    preferably public CA
  - forward the rest transparently (!)
- Monitoring

…

eduroam in a nutshell (2)

- Logging
- Quarantaine
- IPv6
- VLANs
- Guests, eVA
- eduroam CAT, installers

eduroam has proven to be the standard for wireless in edu!

value for the end-users

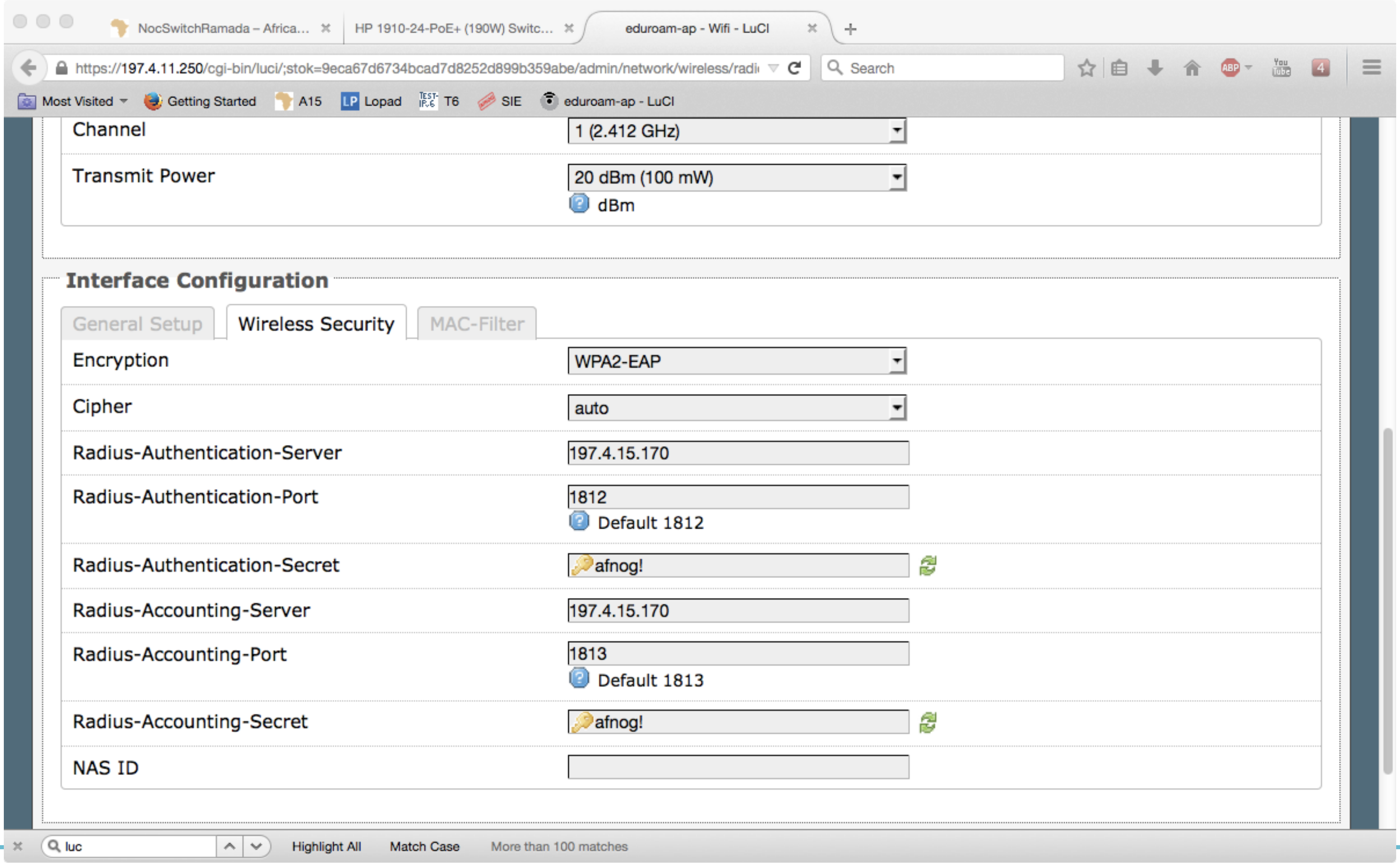
Demonstration

- The access point `‘eduroam-demo’` is connected to a single RADIUS-server
  - No confederation, sorry guys
- Set up some test accounts:

```
user1    Cleartext-Password := "pass1"
user2    Cleartext-Password := "pass2"
user3    Cleartext-Password := "pass3"
user4    Cleartext-Password := "pass4"
user5    Cleartext-Password := "pass5"
user6    Cleartext-Password := "pass6"
user7    Cleartext-Password := "pass7"
```

- Experiment!

AP configuration example


NocSwitchRamada – Africa...
HP 1910-24-PoE+ (190W) Switc...
eduroam-ap - Wifi - LuCI
https://197.4.11.250/cgi-bin/luci/;stok=9eca67d6734bcad7d8252d899b359abe/admin/network/wireless/radi
Search
Most Visited
Getting Started
A15
Lopad
T6
SIE
eduroam-ap - LuCI
luc
Highlight All
Match Case
More than 100 matches

Channel	1 (2.412 GHz)
Transmit Power	20 dBm (100 mW) dBm

Interface Configuration

General Setup | Wireless Security | MAC-Filter

Encryption	WPA2-EAP
Cipher	auto
Radius-Authentication-Server	197.4.15.170
Radius-Authentication-Port	1812 Default 1812
Radius-Authentication-Secret	afnog!
Radius-Accounting-Server	197.4.15.170
Radius-Accounting-Port	1813 Default 1813
Radius-Accounting-Secret	afnog!
NAS ID	

Questions?

EDUroam contact:
paul.dekkers [at] surfnet.nl