Eduroam CAT

Stefan Winter, RESTENA

TF-Mobility, Internetland, 30 june 2011

What's the CAT?

- Configuration Assistant Tool

- Prerequisiste:
  - IdP lets us know its configuration details:
  - CA, certificate CN(s), EAP types
- Eduroam OT maintains a device database
  - Select devices only
  - Including, but not limited to: which EAP types does device support
- User request on web site:
  - Selects IdP
  - Selects device
  - Either gets a site installer for device, or a “Sorry”
  - Current thinking: extend the “Sorry” to a screenshot walk-through

UI

Two-faced web interface

- IdP “interview” style upload of config details
  - *Enables us to let know of inconsistencies*
  - *Will only generate installers if **complete** info is submitted*
- User “what's your inst and device?” drop-down

IdP interface

- Institution can have multiple profiles
- Profile can support multiple EAP-Types
  - *IdP selects preference of types*
- IdP can upload branding
- Logos
- Disclaimer texts to show during install; selected devices only

IdP configuration details

- Why profiles?
  - Students vs. Staff
  - Different EAP-Types
  - Different helpdesks?
  - Different CAs?
  - Different Auth Servers → Different Cns?
  - To prevent “Lost in option bloat”: EAP properties can be set on per-IdP level, which applies to all profiles and EAP types; we expect this to be the most common use

- Why EAP preferences? Scenarios:
  - Students with PEAP (preferred) and TTLS
  - Staff with TLS (preferred) and PEAP
  - e.g. if a device doesn't support “the” EAP type

While we're at it...

This is the first time we are in direct contact with IdPs

They want something from us, so we can go on their nerves :-)

- Nag about anonymous outer identity; suggest that they turn it on
- Inform about importance of CA and CN validation
- Let them know about TTLS-GTC if they don't support anything MS-CHAPv2'ish

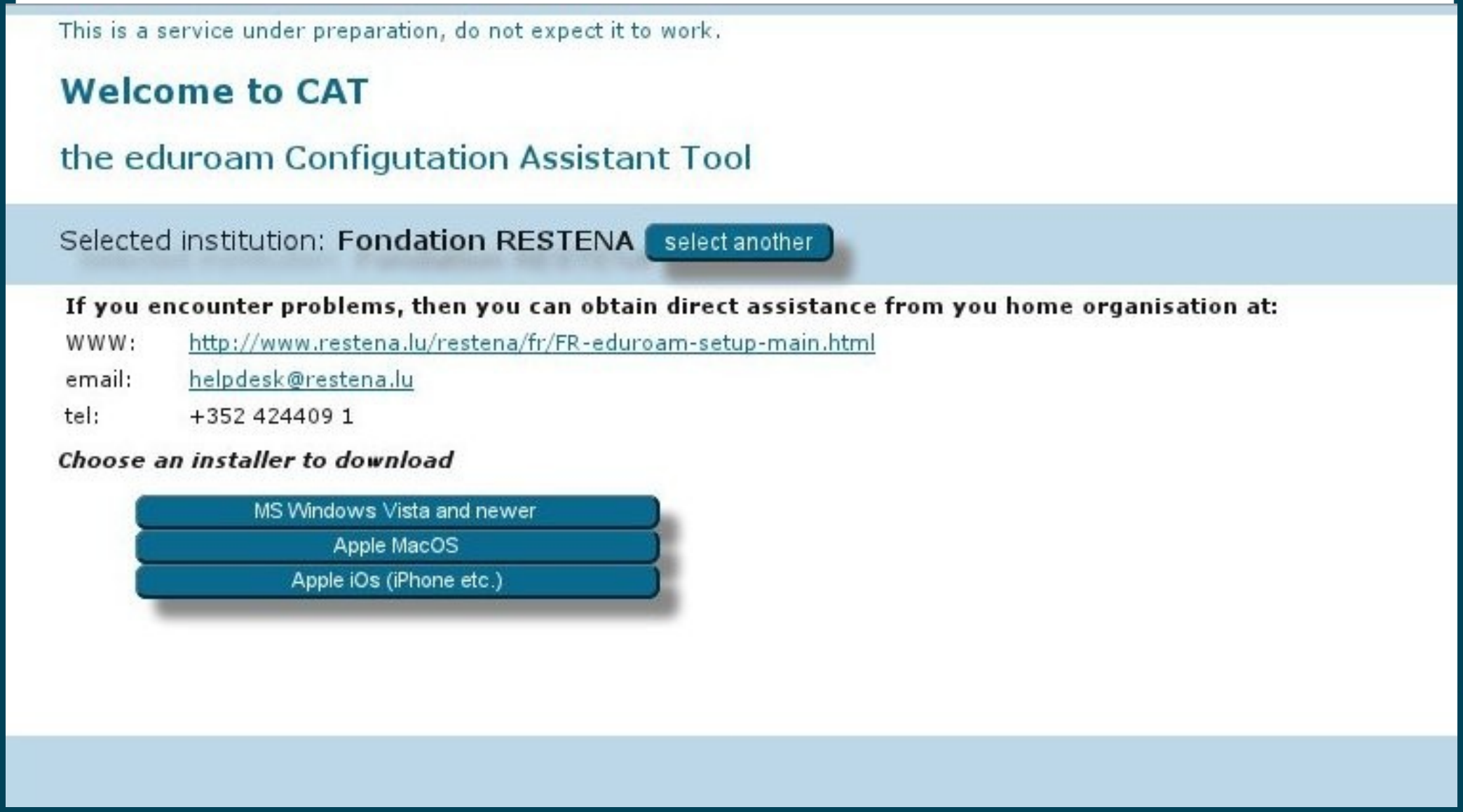
Ideal result: well-educated IdP's all around

IdP configuration details

- Always configures SSID “eduroam” ...
- … but allows to set more SSIDs
- Defaults to WPA2/AES ...
- … but allows to configure a WPA/TKIP profile additionally
  - Except on Windows XP
- Multiple CA roots supported – to make rollover easier

End-user interface demo (Screenshot as fallback)

http://leopard-www.uci.umk.pl/CAT/



General Information

This is the place where you can desribe your institution in a fine-grained way. The solicited information is used as follows:

- **Primary Langauge**: when your users download the installer, we will by default suggest this language to them. All other langauges are selectable though; which is probably beneficial for end users whose mother tongue is not your country's. If you don't specify the default language, the default will be the end user's browser language setting.
- **Logo**: When you submit a logo, we will embed this logo into all installers where a custom logo is possible. We accept any image format, but for best results, we suggest SVG. If you don't upload a logo, we will use the generic eduroam logo instead.

General: Primary Language [ ] Delete

General: URL to logo [ ] Delete

Add new option

Location

The user download interface (see here), uses geolocation to suggest possibly matching IdPs to the user. The more precise you define the location here, the easier your users will find you.

- Drag the marker in the map to your place, or
- enter your street address in the field below for lookup, or
- use the "Locate Me!" button

We will use the coordinates as indicated by the marker for geolocation.

Address: [ ] Do something! Locate Me!

Latitude: 49.815273 Longitude: 6.129583

Helpdesk Details for all users

If your IdP provides a helpdesk for its users, it would be nice if you would tell us the pointers to this helpdesk. Some site installers might be able to signal this information to the user if he gets stuck.

If you enter a value here, it will be added to the site installers for all your users. If you operate separate helpdesks for different user groups (we call this 'profiles'), or operate no help desk at all (shame on you!), you can also leave any of these fields empty and optionally specify per-profile helpdesk information later in this wizard.

Support: E-Mail [ ] Delete

Support: Web [ ] Delete

Support: Phone [ ] Delete

Add new option

EAP details for all users

Most EAP methods need server-side authentication details, like the CA certificate and/or server name(s) of your authentication servers. If all the EAP methods you support work with the same CA and or Common Names of servers, you can enter them here and they will be added as trust anchors in all profiles. If the details differ per profile or per EAP-type, you can also enter them in the individual profiles later.

Note well: The server-side validation is a cornerstone of eduroam; without it, users are subject to man-in-the-middle attacks! We will not generate site installers without Trusted CA anchors and server names.

URL to CA Certificate [ ] Delete

Name of Authentication Server [ ] Delete

Add new option

When you are sure that everything is correct, please click on Continue ...

eduroam Configuration Assistant Tool (CAT)
IdP Configuration Interface

Preprodwarning: This is a prototype. Don't complain if it creates disruptions in the space-time continuum!

Identity Provider Overview

IdP-wide settings

General Institution Details

Country: **lu**
Institution name: **Foobar, Inc.**
Primary Language: **xy**

Global Helpdesk Details

Support: Web **http://foo.bar**
Support: Phone **+352 12345**
Support: E-Mail **foobar@inc**
Support: Phone **+123 456 789**
Support: E-Mail **foonet@skynet**

Global EAP Options

URL to CA Certificate **http://www.eduroam.lu/certs/cacert.pem**
Name of Authentication Server **eduroam.restena.foobar**

Profiles for this institution

Profile: blablub1

EAP Types (in order of preference):
TTLS-PAP OK
TTLS-GTC OK
Edit Delete

Profile: blablub2

EAP Types (in order of preference):
TTLS-PAP OK

Read this tip.

Edit Delete

Profile: blablub3

EAP Types (in order of preference):
PEAP-MSCHAPv2 OK
EAP-TLS OK
Edit Delete

Profile: foobarsnettet

EAP Types (in order of preference):
PEAP-MSCHAPv2 OK
TTLS-MSCHAPv2 OK
Edit Delete

Profile: nexttry

EAP Types (in order of preference):
EAP-FAST-GTC Information needed!
EAP-TLS OK
Edit Delete

Profile: yetanotherprofile

EAP Types (in order of preference):
TTLS-PAP OK

Read this tip.

Edit Delete

Add new profile ...

Device database

- Contains
  - Supported EAP types
  - Unsupported EAP types
  - (implicit: “We don't know” EAP types)
  - Caveats
    - *“No anonymous identity on this platform”*
    - *Etc.*

- When user selects inst profile and device:
  - Go through IdP's EAP type list in desc order of pref
  - Check if device supports this EAP type
  - On first match, generate config stuff
  - (not yet clear: if less-preferred has site config, use that instead?)
  - If no match, “Sorry” - or smart(?) advice like for TTLS-GTC

Internationalisation

Internationalisation

- We'll do the thing in English, but with i18n() calls built-in
- Hope to get other NRENs in for translation
- You could get a UK Uni's installer in French, Slovenian, or whatever for those students with non-English background!

On user-facing side, let user choose

- IdP sets “default” language
- User can override (maybe using browser default language settings?), and gets installer in his language of choice (if i18n'ed already)

User-facing GUI

- “WAYF” needed when user selects institution
- Drop-down lists for the beginning, but maybe we can learn from the SAML people

Devices to-be-supported

Microsoft Windows

- XP (SecureW2, if still needed)
- Vista (PEAP+TLS with netsh, TTLS with SecureW2)
- 7 (PEAP+TLS with netsh, TTLS with SecureW2)

Apple

- i* devices (mobileconfig)
- OS X Lion (also mobileconfig)
- OS X <Lion (plist; but will only do this if installed base post-Lion release warrants the effort)

Linux

- wpa_supplicant
- Plans for KnetworkManager; vague right now

Devices to-be-supported(2)

Android

- Vague plans; Android app envisaged

Nokia

- Screenshots maybe

Windows Mobile

- Screenshots maybe