

eduroam service status

Miroslav Milinović
University Computing Centre – Srce
Zagreb, Croatia
<miro@srce.hr>

Marseille, February 6, 2008



eduroam service

- ❖ eduroam user experience: “open your laptop and be online”
- ❖ to provide secure network access inside the confederation boundaries (to the end users)
- ❖ eduroam is a secure international roaming service for members of the European eduroam confederation (a confederation of autonomous roaming services)

eduroam service elements

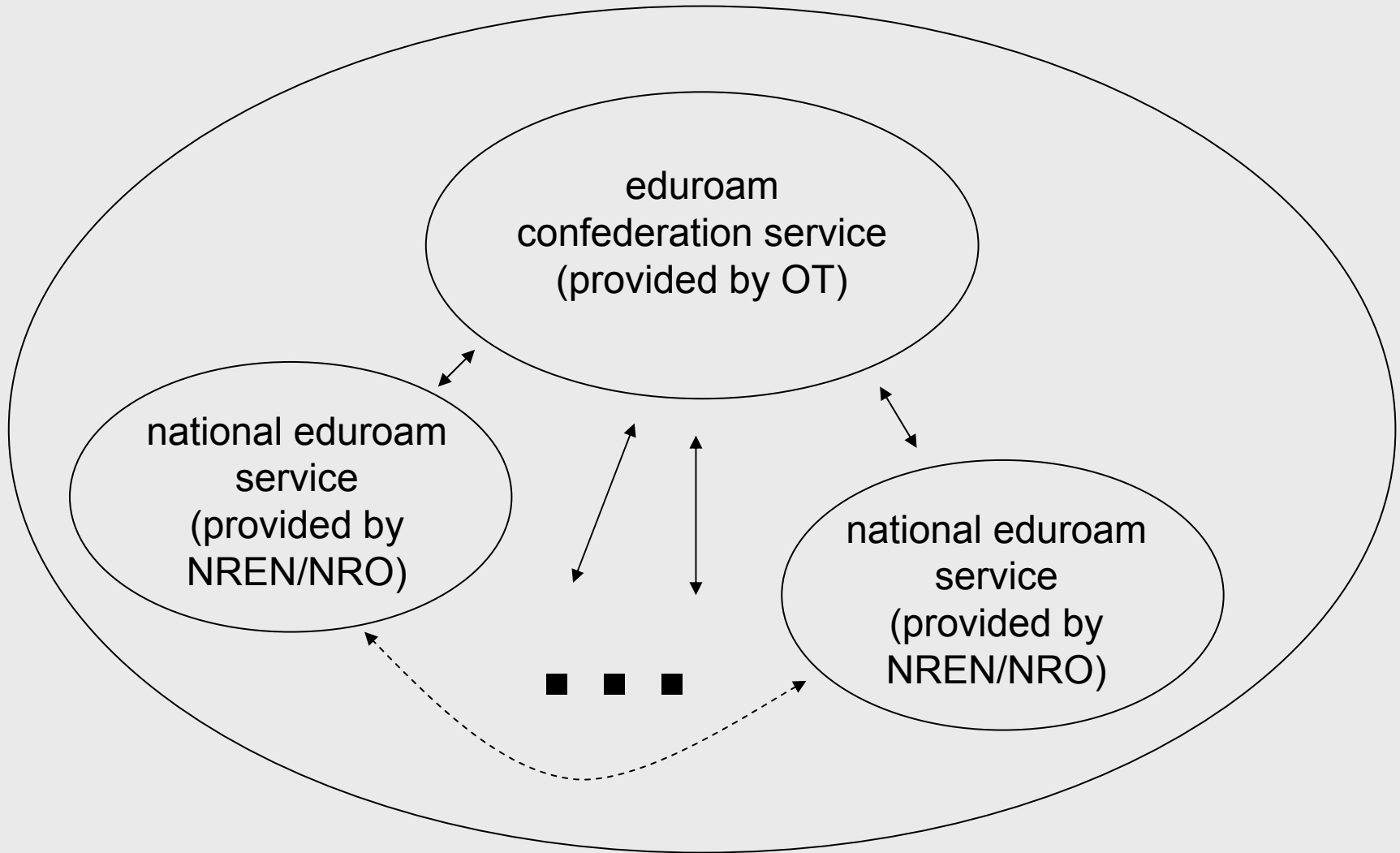
- ❖ technology infrastructure
- ❖ supporting infrastructure
 - ◆ monitoring and diagnostics
 - ◆ eduroam web site
 - ◆ eduroam database
 - ◆ trouble ticketing system (TTS)
 - ◆ mailing lists

Users vs. service elements

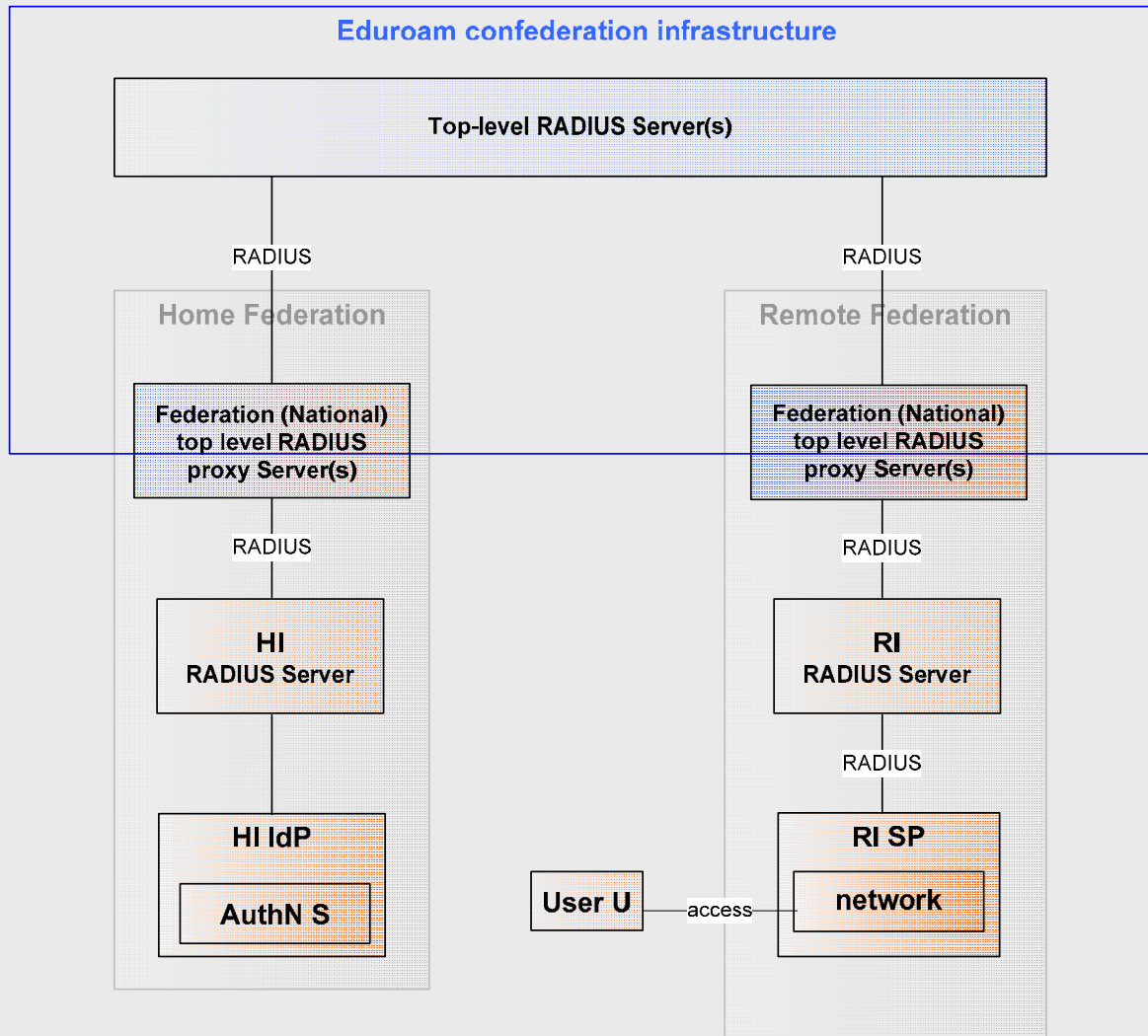
Service elements	User group		
	End user	Inst. Level personnel	Federation-level personnel
Basic monitoring facilities	Yes	Yes	Yes
Full monitoring and diagnostics facilities	No	Yes (limited to the information regarding the respective inst.)	Yes
Public access to the eduroam web site	Yes	Yes	Yes
Access to the internal eduroam web site	No	Yes (limited to the information regarding the respective inst.)	Yes
Public access to the eduroam database	Yes	Yes	Yes
Access to the all information in the eduroam database	No	Yes (limited to the information regarding the respective inst.)	Yes
TTS	No	Yes	Yes
SA5/OT Mailing lists	No	No	Yes
Support form OT	No	No	Yes

Eduroam service model

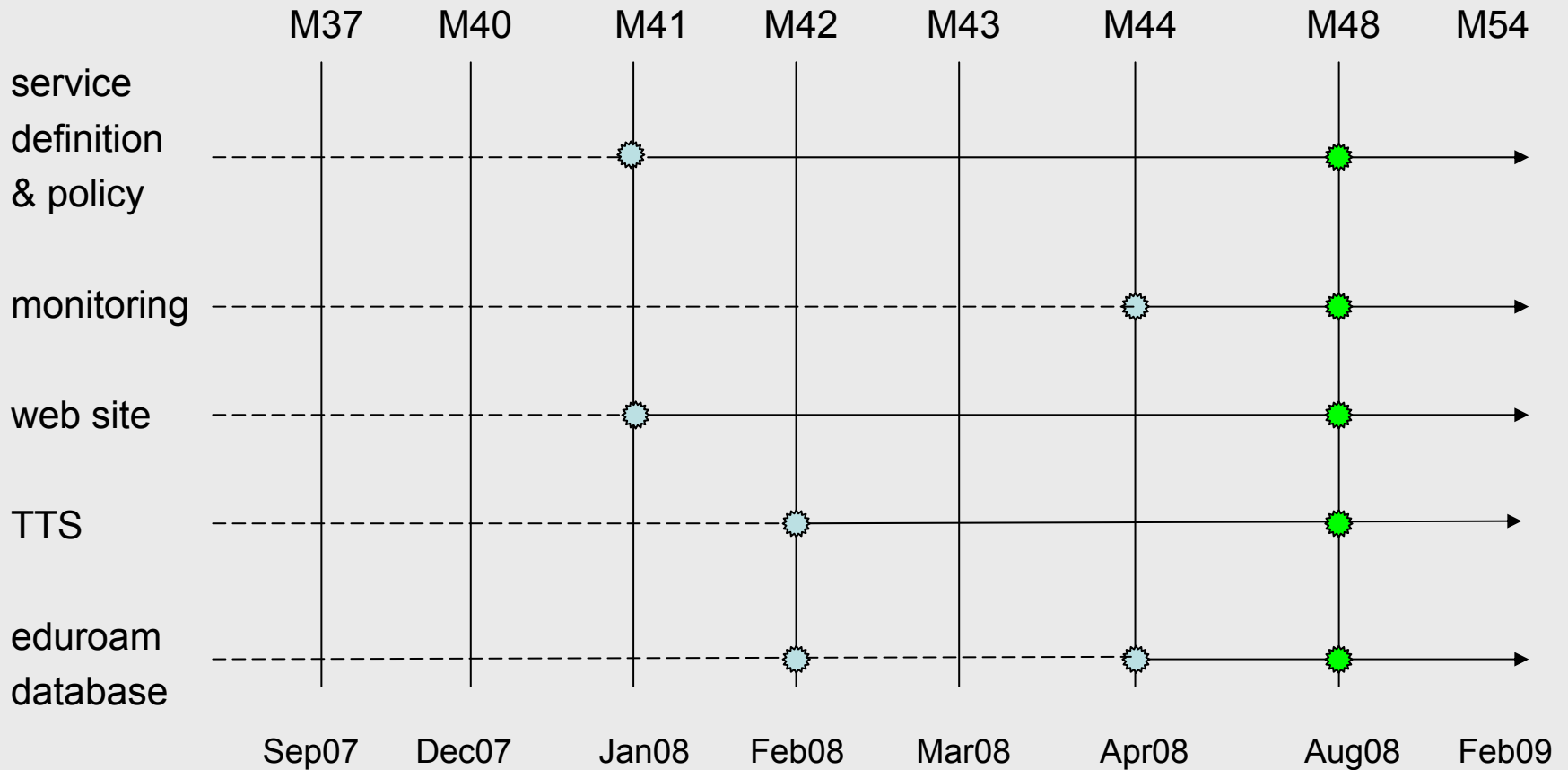
eduroam service (governed by SA5)



eduroam infrastructure



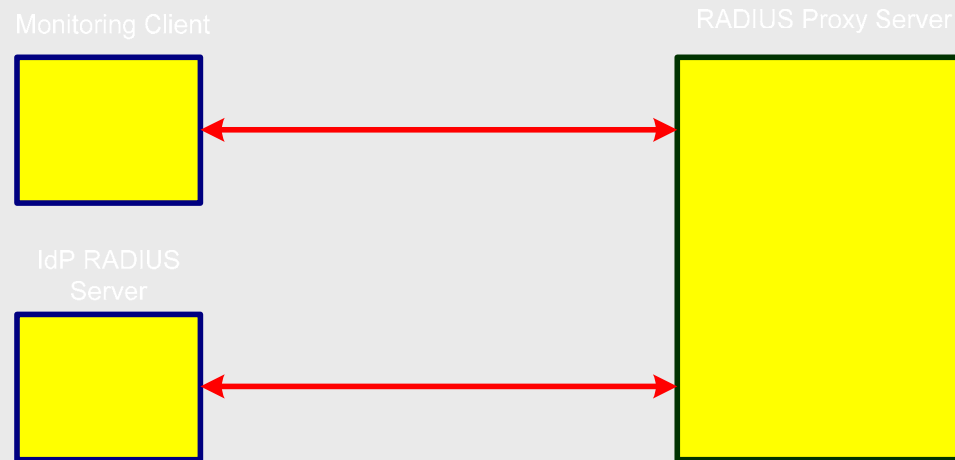
Implementation plan



Monitoring: problem definition

- ❖ monitor functionality of the eduroam infrastructure
 - ◆ servers
 - ◆ infrastructure
 - ◆ user experience
- ❖ it is not enough to know that host is accessible

Monitoring: concept



- ❖ **Monitoring client** is RADIUS client capable of sending various types of RADIUS request (PAP, EAP, ...)
- ❖ **RADIUS Proxy Server** is monitored server
- ❖ **IdP RADIUS Server** is the server that issues the response thus acting as loop-back server. It's function is to close the tunnel and create standard well format and specified response. This function might be realized on the monitored server (RADIUS proxy server)

Monitoring: process

- ❖ Monitoring process is performed in two steps REJECT test and ACCEPT test
- ❖ Both steps include :
 - ◆ Monitoring client creates RADIUS attributes specific for monitoring purpose
 - ◆ Monitoring client creates RADIUS request based on selected AuthN type (now EAP/TTLS)
 - ◆ Monitoring client sends RADIUS request, and starts measuring response time
 - ◆ Monitored RADIUS Proxy Server handles request and sends back the response
 - ◆ Monitoring client evaluates received response and updates database.
 - ◆ Monitored server is marked OK if it fulfills both testing steps.

- ❖ Monitored data, saved in database:
 - ◆ is monitoring request accepted by RADIUS proxy server ? (yes/no)
 - ◆ is request properly routed? (currently to eduroam.<tld>)
 - ◆ type of RADIUS request (currently only EAP/TTLS)
 - ◆ is response well formed (equal to expectations)?
 - ◆ response time

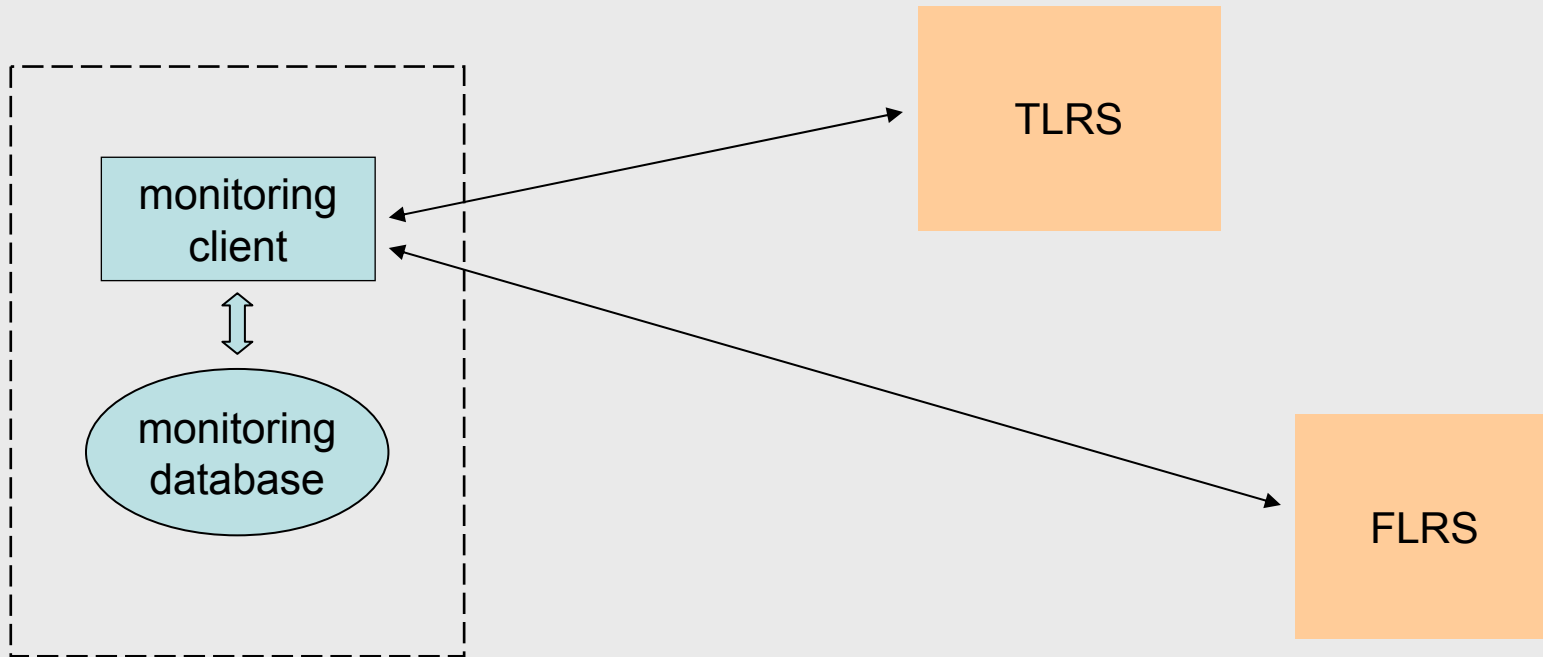
Monitoring: why do we need “accept logic” tests?

- ❖ there are limits on sending Reply-Message with Reject (RFC3579 forbids Reply-Message attribute when EAP-Message is in the packet)
- ❖ are we testing real user experience?
 - ◆ currently collected data shows differences
 - ◆ (very) different workflows at RADIUS servers for Accept and Reject

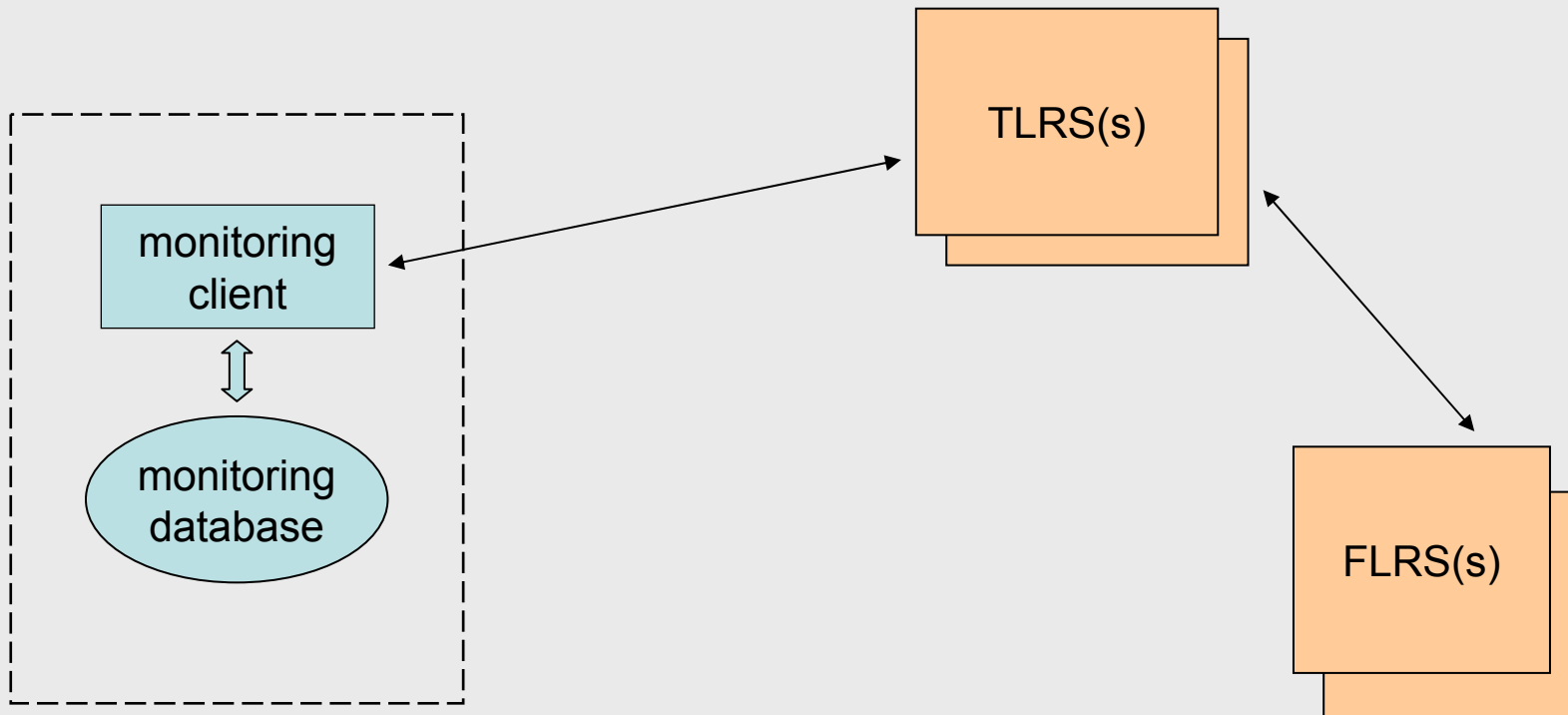
Monitoring: security?

- ❖ Following attributes are used in creating RADIUS request (both for REJECT and ACCEPT test):
 - ◆ NAS-IP-Address = 161.53.2.204 (IP address of monitoring client)
 - ◆ NAS-Port = 8484
 - ◆ Calling-Station-Id = eduroamMON
 - ◆ Called-Station-Id = eduroamSCH
 - ◆ NAS-Identifier = SA-EAP-TTLS
 - ◆ Connect-Info = eduroam-monitoring
- ❖ Password for the testing user is known only by the monitoring client and can be generated on the fly for each monitoring session

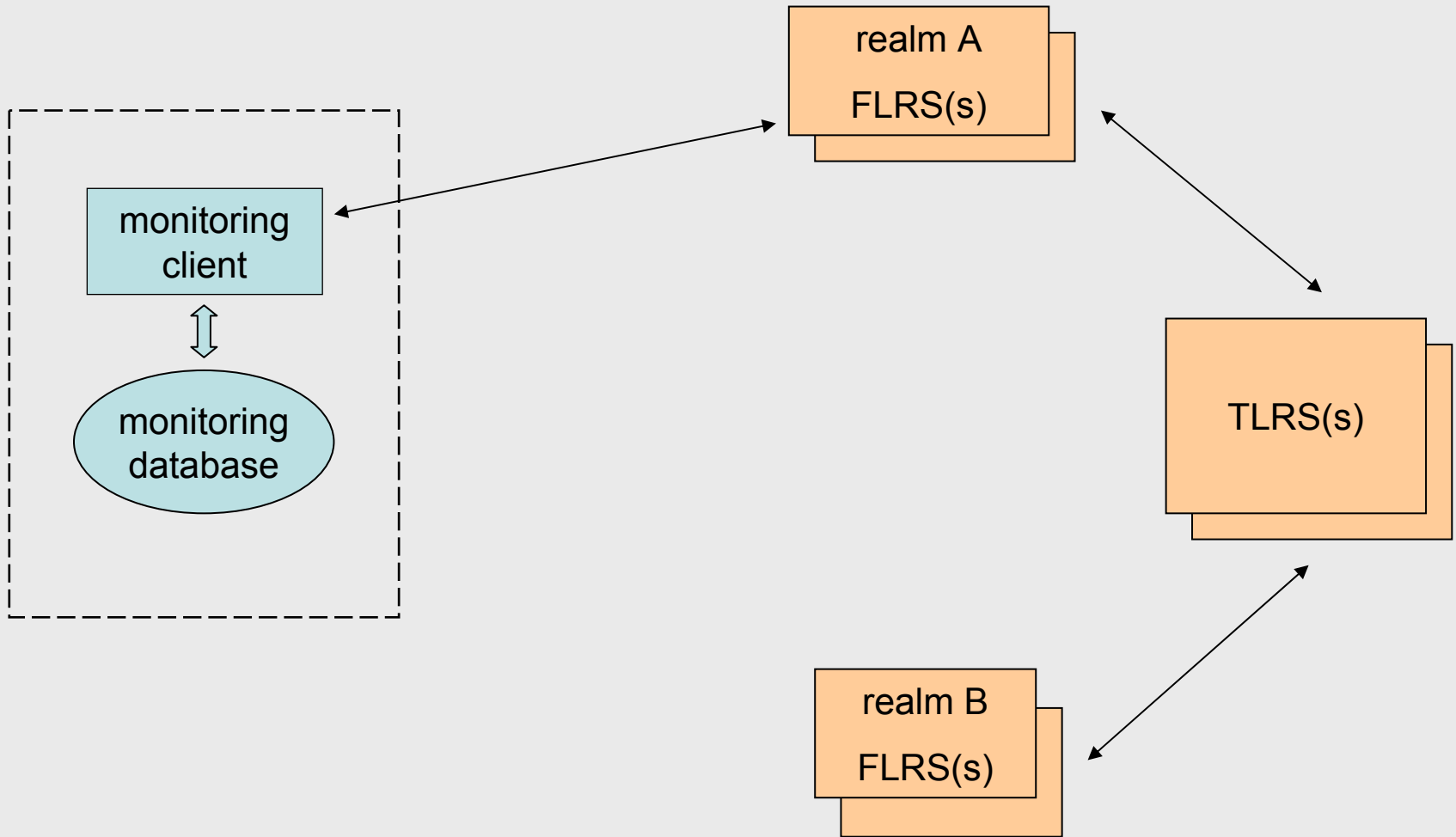
Monitoring servers



Monitoring infrastructure



Testing on demand



Monitoring: implementation status

- ❖ monitoring client & database
 - ♦ works well
 - ♦ to do:
 - add RadSec functionality; (EAP/TLS ?)
 - better web pages
 - public and internal part (Auth via eduroam or eduGAIN ?)
- ❖ pilot service (<http://wcon.srce.hr/eduroam/>)
 - ♦ monitoring servers (running)
 - ♦ monitoring infrastructure (just started)
 - ♦ testing on demand (to be finalised)
- ❖ full production
 - ♦ NAGIOS framework
 - ♦ new HW, final set-up

eduroam database

- ❖ The information stored in the eduroam database includes:
 - ♦ NRO representatives and respective contacts
 - ♦ Local-institutions (both SP and IdP) official contacts
 - ♦ Information about eduroam hot spots (SP location, technical info)
 - ♦ Monitoring information
 - ♦ Information about the usage of the service
- ❖ NROs:
 - ♦ should provide respective data (general and usage data)
 - ♦ in the defined XML format
 - ♦ available at the specified URL (<http://www.eduroam.<tld>/usage/> , <http://www.eduroam.<tld>/general/>)
 - ♦ should be accessible only from the eduroam database server

eduroam database (v.0.5)

