TCS 4 RadSec

Milan Sova
Objective?

- Let's accredit TCS under the eduroam Trust profile as defined by eduPKI.

and

- use the *established* and *commonly accessible* PKI
Issue 1: Trust

Addtrust External Root CA

UTN-USERFirst-Hardware

TERENA SSL CA

RadSec1  RadSec2  RadSecN

Other Intermediate CA

Yet Another Foreign CA

Other Foreign CA

Host1  Host2
Issue 2: Certificate Profile

- Policy OIDs for eduroam SP/IdP
Issue 3: TCS vs. eduroam policy

- A Requester SHALL be identified by his/her email address verified and asserted by the corresponding eduroam® National Roaming Operator.

- A Requester MUST prove to the CA its entitlement to operate a RADIUS/TLS service participating in eduroam®. The entitlement MUST be approved by the eduroam® NRO.
Solutions?
Issue 1: Trust

Addtrust External Root CA

UTN-USERFirst-Hardware

TERENA SSL CA

RadSec1  RadSec2  RadSecN

Other Intermediate CA

Yet Another Foreign CA

Other Foreign CA

Host1  Host2
Remedy 1: Trust

eduroam Root CA

Addtrust External Root CA

UTN-USERFirst-Hardware

Other Intermediate CA

Yet Another Foreign CA

Other Foreign CA

TERENA SSL CA

RadSec1  RadSec2  RadSecN

Host1  Host2
Issue 2: Certificate Profile

- Policy OIDs for eduroam SP/IdP
Remedy 2: Certificate Profile

- Policy OIDs for eduroam SP/IdP
- COMODO can deploy new certificate profiles
Issue 3: TCS vs. eduroam policy

- A Requester SHALL be identified by his/her email address verified and asserted by the corresponding eduroam® National Roaming Operator.

- A Requester MUST prove to the CA its entitlement to operate a RADIUS/TLS service participating in eduroam®. The entitlement MUST be approved by the eduroam® NRO.
Issue 3: TCS vs. eduroam policy

- A Requester SHALL be identified by his/her email address verified and asserted by the corresponding eduroam® National Roaming Operator.

- A Requester MUST prove to the CA its entitlement to operate a RADIUS/TLS service participating in eduroam®. The entitlement MUST be approved by the eduroam® NRO.

- Change TCS procedures
Change TCS procedures

vs.

• „use the *established* and *commonly accessible* PKI“