



eduroam-ng

Milan Sova
sova@cesnet.cz

Stávající architektura

- RADIUS
 - lokační služba
 - zdroj důvěry
 - transport

Problémy

- spojení bod – bod
 - zabezpečení
 - škálování
- RADIUS
 - zabezpečení
 - UDP
 - minimální autorizace

Nová architektura - požadavky

- oddělení
 - IS
 - mechanismů zajištění důvěry
 - transportu
- autorizace

Informační služba

- lokační služba
- podpora sítě důvěry
- podklady pro monitoring

- distribuovaná
- hierarchická

- DNS(SEC), LDAP...

Sít' důvěry

- vzájemná důvěryhodnost jednotlivých prvků infrastruktury
- distribuovaná?
- hierarchická?
- DNSSEC, X.509 PKI...

Transport

- zabezpečený kanál uživatel – domovská autentizační služba
- spojení
 - 1) přímé
 - 2) s využitím stávající hierarchie
- možnost připojení RADIUS zařízení
- DIAMETER, SOAP/SAML...

eduroam-ng – *varianta I*

- DNSSEC, IPsec, RADIUS
 - lokace AA služeb v DNSSEC
 - veřejné klíče AA serverů v DNSSEC
- implementace DNSSEC resolveru
- pomalé navazování IPsec spojení

eduroam-ng – *varianta II*

- DNS, X.509 PKI, DIAMETER
 - lokace AA služeb v DNS
 - důvěryhodné CA
 - DIAMETER (IPsec, TLS)
- implementace DIAMETER

eduroam-ng – *varianta ...*

- kombinace technologií z předchozích variant
- nové technologie...

Autorizace

- syntaxe a sémantika atributů
- transport autorizačních dotazů a odpovědí
 - 1) autentizační trasportní protokol
 - 2) jiný autorizační systém (Shibboleth, PAPI...)

eduroam-ng

- TERENA TF-Mobility
- AARNET
- Internet2 FWNA

eduroam-ng

???