cesnet

DIGITÁLNÍ IDENTITY

Jiří Bořík
CESNET

konference e-infrastruktury CESNET 2019
Praha

OBSAH PREZENTACE

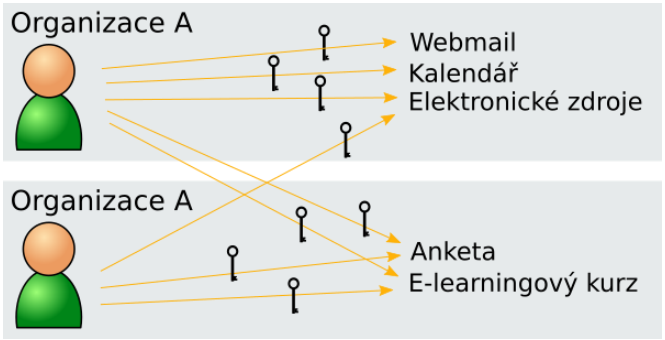
- fyzická a elektronická identita
- federace eduroam
- federace eduID.cz
- elektronické certifikáty a PKI služby
- eIDAS
- správa identit a přístupů = Perun

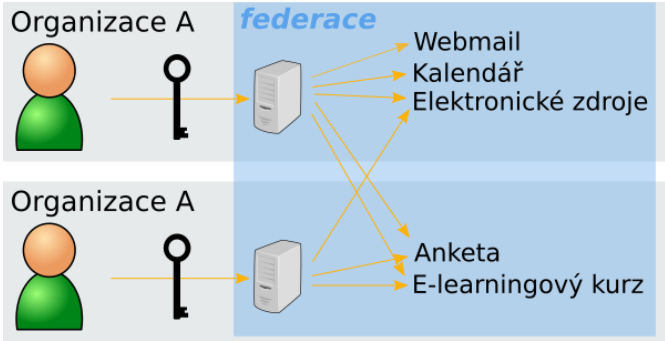
FYZICKÁ A ELEKTRONICKÁ IDENTITA

- **Identita**
  - Fyzická x elektronická
  - Lokální x federovaná
- **Důvěryhodnost - spolehlivé a bezpečné ověření**
  - Původ - domovská organizace (statutární orgán, IdP)
  - Nezávislá třetí strana (OP, pas, certifikáty)
- **Ochrana soukromí**
  - Zneužití dat identity, podvržení identity
  - Ochrana citlivých dat nejen z hlediska GDPR
  - Bezpečný provoz služby
- **Snadnost použití**
  - Různé ověřovací prostředky pro různé účely
  - Možnost výběru preferovaného způsobu (silně ověřená identita x sociální sítě)

FEDERACE IDENTIT

- **Operátor federace**
  - Provozuje centrální infrastrukturu federace
  - Komunikuje s nadřazenými interfederacemi
  - Určuje pravidla (komunitní vyjednávání)
- **Federační politika**
  - Deklarace účelu federace (zaměření, komunita)
  - Administrativní a provozní pravidla
- **Poskytovatel identity**
  - Garantuje ověření uživatele
  - Může poskytnout o uživateli doplňující informace
- **Poskytovatel služby**
  - Nabízí službu definovaných vlastností
  - Garantuje řádnou manipulaci s uživatelskými daty
  - Pro některé služby potřebuje určit kategorii uživatelů





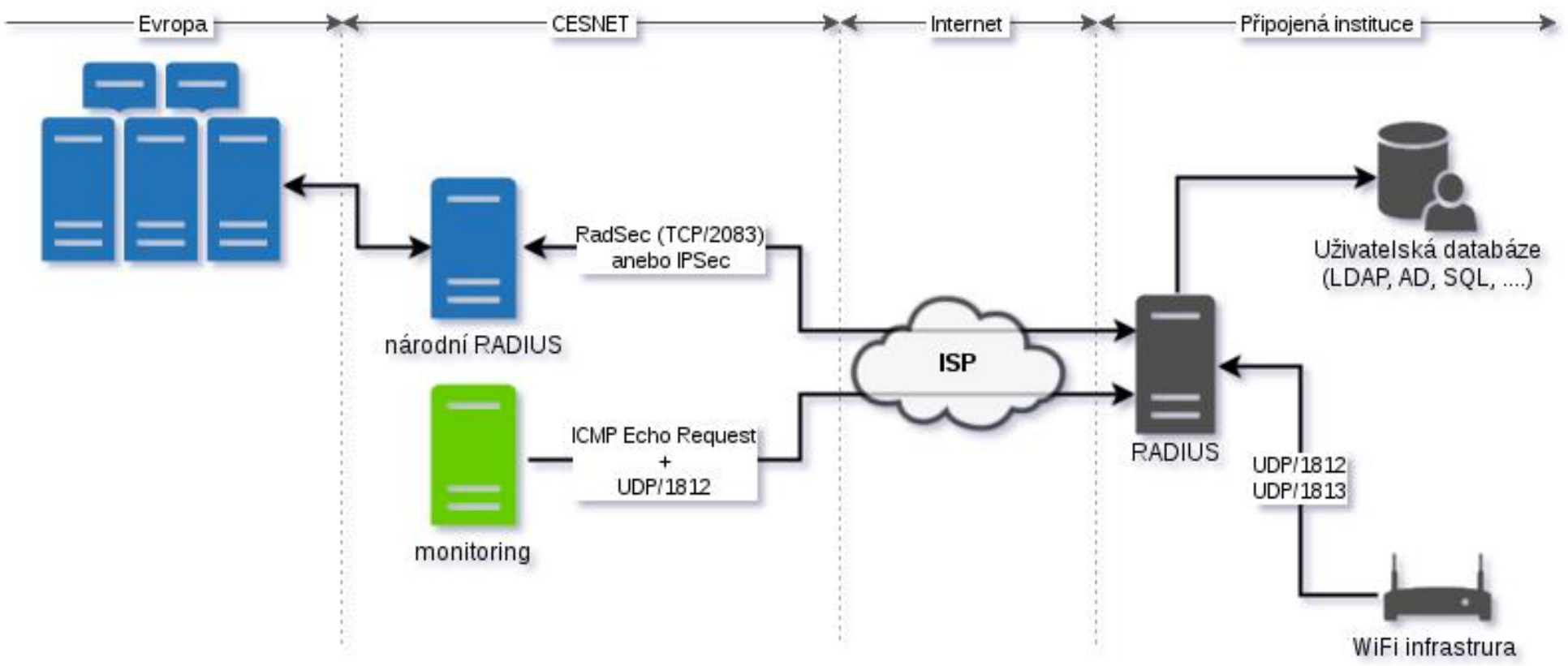
Charakteristika prostředí

- Jedna jasně definovaná služba (konektivita), bez omezení a kategorizace uživatelů
- Maximální jednoduchost použití (automatické připojení zařízení, snadná konfigurace - eduroam CAT)
- Přiměřená ochrana soukromí (přístup vyhrazeným jménem a heslem v zařízení, provoz po SSL protokolech, alternativně VPN)
- Reciproční poskytování služby všem uživatelům z členských organizací

Operátor federace = sdružení CESNET

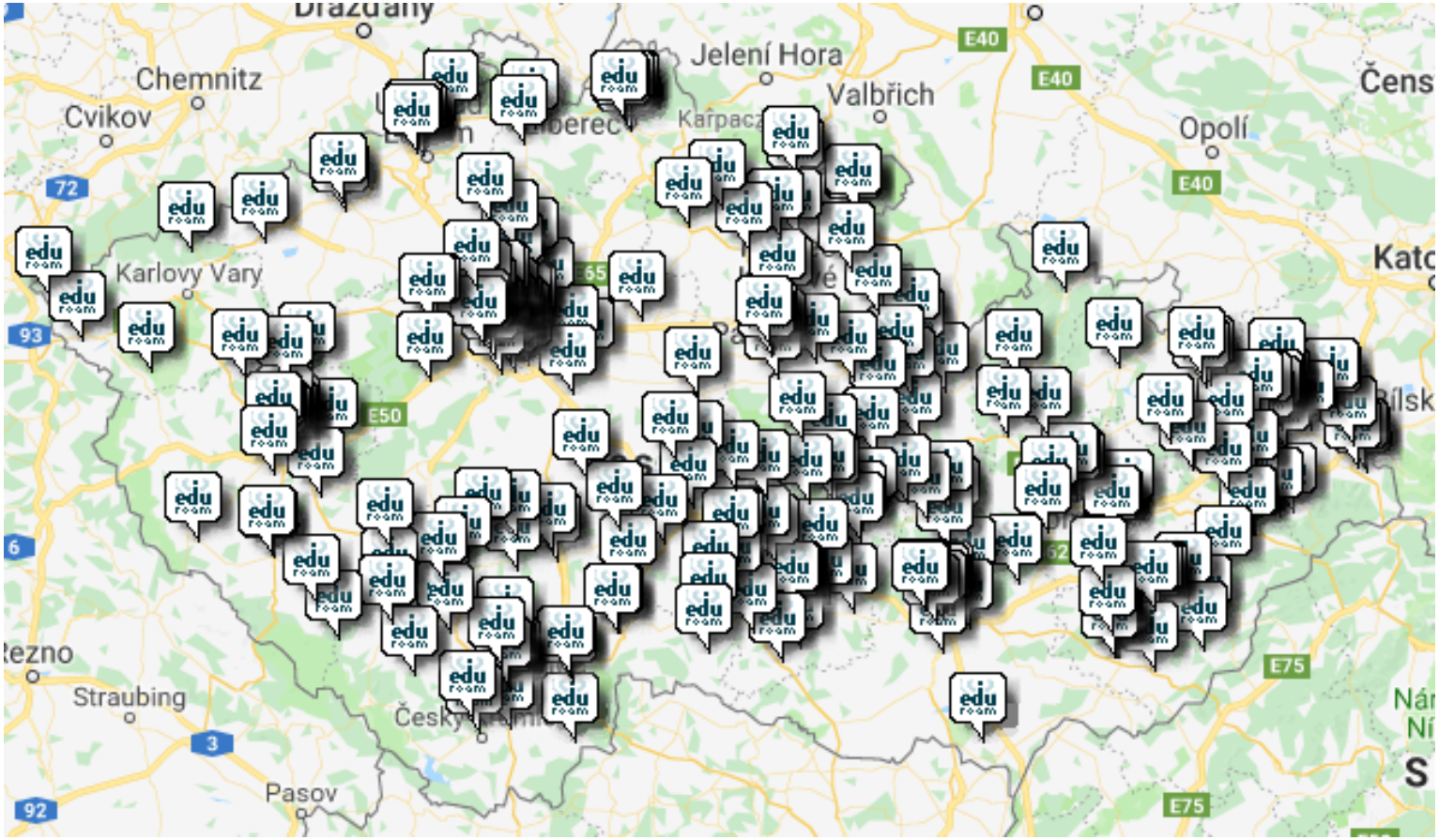
- Provoz národní infrastruktury
- Podpora připojování nových členů
- Podpora adminů členských organizací
- Další podpůrné služby
  - ermon – monitoring prvků sítě všech členů, avizo členům o nefunkčnosti části infrastruktury
  - etlog – statistiky provozu a detekce zneužitých účtů a zařízení
  - RADIUS ve správě CESNETu
  - Podpora automatizované správy freeRADIUSu
  - eduroam AP – pokrytí dočasných prostorů, snadné nasazení

eduroam – PRINCIP FUNKCE



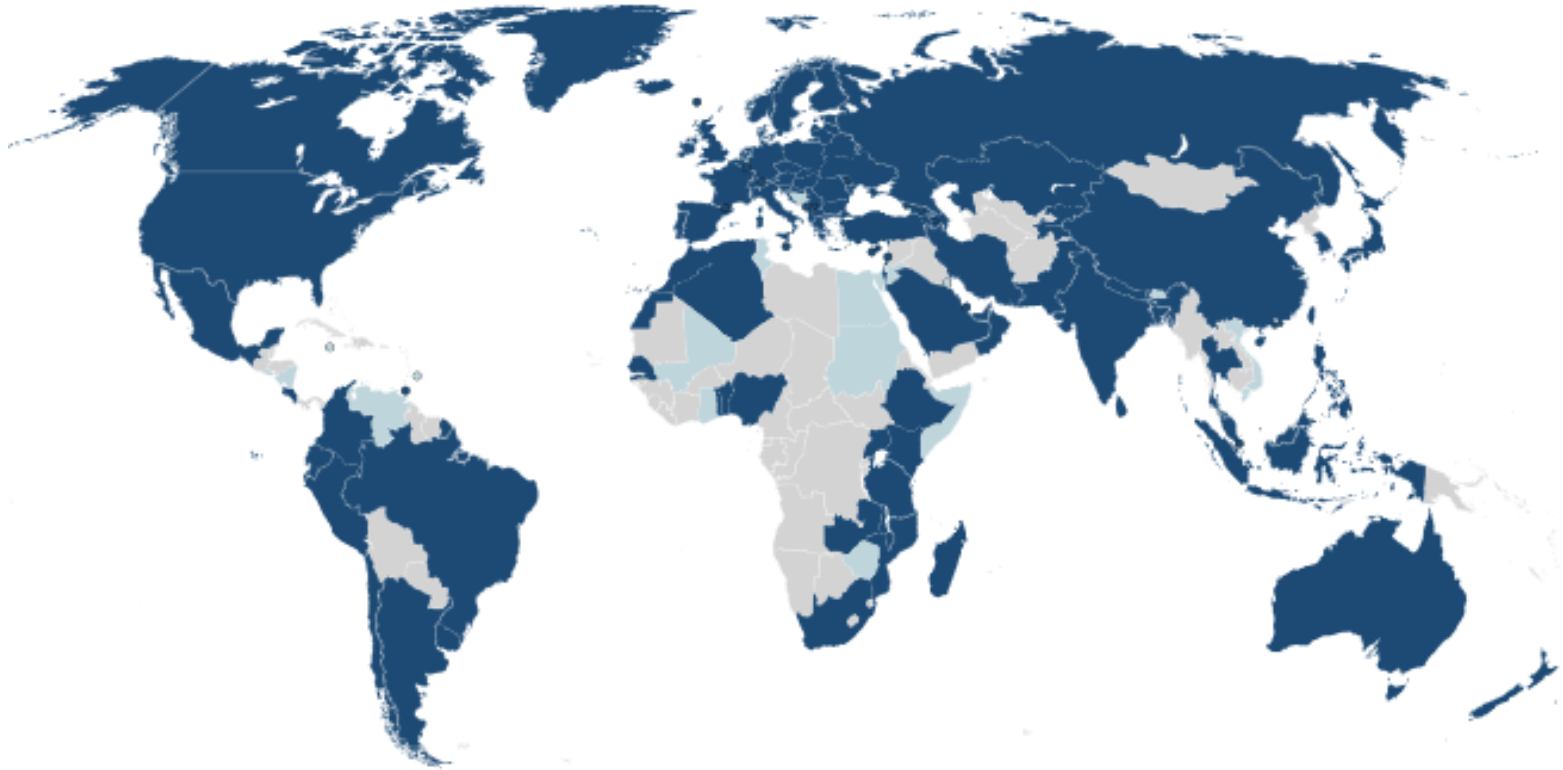
cesnet

POKRYTÍ ČR



cesnet

POKRYTÍ VE SVĚTĚ



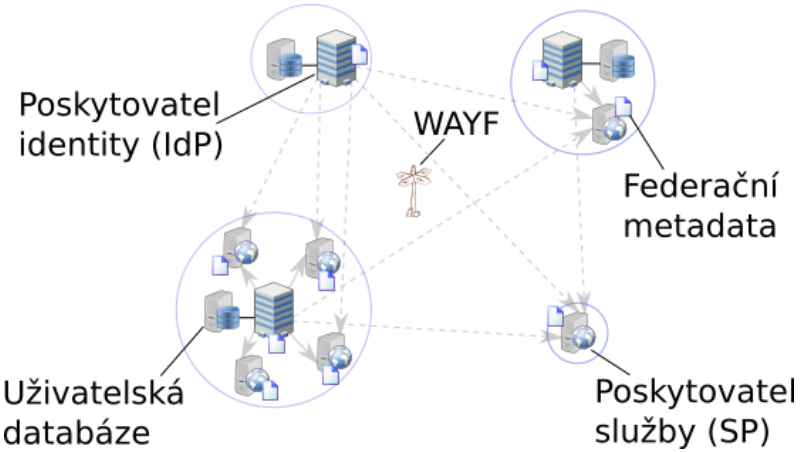
eduroam V ČÍSLECH

- 269 členů (přírůstek nových členů za 2018: 152!)
- přes 900 lokalit
  - AV,
  - VŠ a UNI, střední školy,
  - Veřejné instituce,
  - Nádraží
    - Praha hl. n., Praha Masarykovo, Pardubice, Ústí nad Labem, Hradec Králové, Olomouc, Zlín
    - V plánu: Plzeň, Ostrava hl.n., Ostrava Svinov, České Budějovice, Brno
- eduroam je nejen edu
  - Podmínka členství: splnění zásad pro přístup do Velké infrastruktury CESNET
  - Kromě vědy a výzkumu také
    - Organizace šířící vzdělanost, kulturu a prosperitu
    - Vybrané organizace veřejné správy
    - Kraje (Vysočina, Zlín), Magistráty měst (Plzeň) a další instituce

eduID.cz - PRINCIPY

Charakteristika prostředí

- Různé služby, různé podmínky poskytování (omezení přístupu na určité kategorie uživatelů)
- Přímá komunikace IdP-SP dle metadat federace
- IdP kromě ověření poskytuje i další informace
  - Kategorie organizace, R&S, CoCo, SIRTFI
  - Kategorie uživatele (akademik, student, zaměstnanec, člen)
  - Další osobní údaje dle charakteru služby (jméno, příjmení, e-mail…)



Operátor federace = sdružení CESNET

- Provoz národní infrastruktury (správa metadat, WAYF)
- Podpora stávajících i nových členů
- Komunikace s interfederací eduGAIN

eduID.cz – ČLENOVÉ A SLUŽBY

Členové federace (127 IdP)

- Akademie věd ČR
- Univerzity a vysoké školy
- Výzkumná centra
- Fakultní nemocnice
- Knihovny
- Hostel
- Externí IdP
  - Facebook, GitHub, Google, LinkedIn, mojeID, ORCID
- Zahraniční IdP (eduGAIN)

Poskytované služby (229 SP)

- Elektronické zdroje
- Datová úložiště, ownCloud, FileSender
- Gridová výpočetní infrastruktura
- Podpora spolupráce - Videokonference a webkonference
- Osobní a serverové certifikáty
- Časová razítka
- Vnitřní služby univerzit (omezení služeb jen na určitá IdP)
- Zahraniční služby (eduGAIN)

cesnet

PKI SLUŽBY

CESNET CA3

- Provozujeme vlastní CA a další vyhrazené CA pro různé služby a organizace
- Zajišťujeme provoz a podporu uživatelů
- Podřízené CA na míru

TCS – obecně uznávané serverové a osobní certifikáty

- Zprostředkovaná služba
- Provozujeme lokalizovaný portál a uživatelskou podporu

TSA

- Časové značky
- Provozujeme vlastní TSA servery

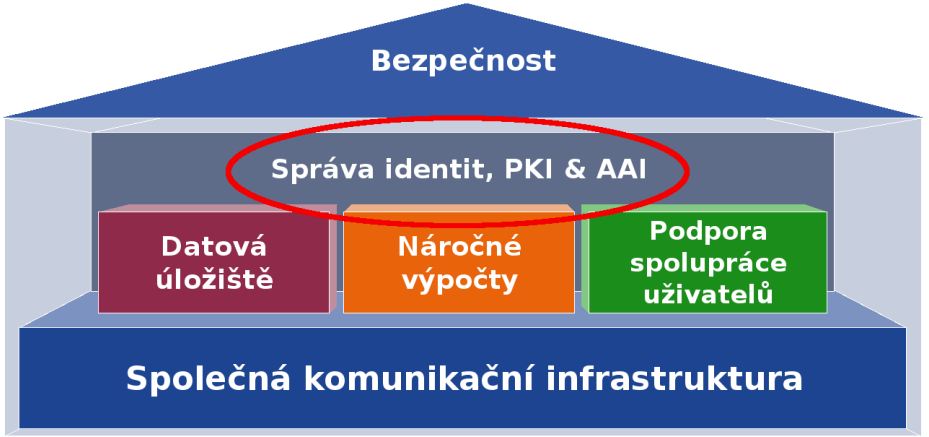
- Kořenová CESNET CA
  - Akreditace u EUGridPMA a eduPKI
- Podřízené CA
  - Možnost nastavení parametrů certifikátů
  - Používá ČVUT, ZČU a projekt Warden
  - Přístup přes Web Services, SAML
- CA není automaticky v prohlížečích a poštovních klientech

- GÉANT Trusted Certificate Service (TCS)
- Certifikační autorita DigiCert
- Certifikáty s obecně uznávanou platností, např. v prohlížečích
- Vydávané typy certifikátů
  - Serverové (OV, EV)
  - eScience serverové
  - eScience osobní
  - Aplikační (Code Signing)
  - Dokumentové
  - Robotové

CESNET a eIDAS

- nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu
- V akademickém prostředí se přímo dotýká především VVŠ, v rámci jejich role Orgánu veřejné moci
- V roce 2019 zahájen společný projekt CESNETu a univerzit pro přípravu vybraných eIDAS služeb, především:
  - Centrální úložiště kvalifikovaných certifikátů
  - Validace podpisů na elektronických dokumentech
- Více informací zítra v sekci Digitální identity a na novém webu eidas.cesnet.cz

- Systém pro správu
  - Uživatelů
  - Skupin
  - Zdrojů
  - Služeb
  - Přístupů
- Vlastnosti
  - Podpora LDAP, AD, SQL, XML, CSV, VOMS
  - Spojování identit
  - Synchronizace s externími systémy
  - Notifikace
  - Auditování



PERUN – NASAZENÍ

Provoz systému Perun

- Bázová IdM služba pro CESNET, MU, VŠUP
- Integrální součást e-infrastruktury CESNET, přístup k jejím službám
- Podpora vědeckých komunit
- Zapojení do mezinárodních projektů (EGI, Elixir, AARC2, EOSC-hub a GN4)

Dostupné platformy pro provoz

- Virtuální skupiny v hlavní instanci e-infra CESNET
- Vlastní instance na zdrojích CESNET
- Vlastní instance na zdrojích uživatele (VŠUP)
- Vyhrazená instance součástí projektu eduTEAMS
- Přístup do testovací instance

Timestamp: '2019-01-27 14:47:10.197'
USERS: '33586'

PERUN V ČÍSLECH

Celkem 8 instalací

- Hlavní instance pro e-infrastrukturu CESNET
- Vyhrazené instance pro mezinárodní projekty
- MU, VŠUP lokální instalace
- Testovací, vývojová

Hlavní instalace CESNET

- Timestamp: '2019-01-27 14:47:10.197'
- USERS: '33586',
- VOS: '324',
- RESOURCES: '2410',
- GROUPS: ‘2081'

cesnet

POZVÁNKA NA ZÍTŘEK

Sál 3: Digitální identity

- **9:30-11:00 Novinky AAI**
  - eduroam a IROP, proxy IdP v e-infra, elektronický občanský průkaz, QR kódy v autentizaci
- **11:30-13:00 eIDAS a VVŠ**
  - Analýza dopadů eIDAS, případová studie, služby CESNET pro eIDAS, vzdálené podepisování
- **14:00-15:30 Knihovní systémy a eduID.cz**
  - Projekt AARC2 a knihovny, portál Knihovny.cz, CzechELib, BOOKPORT
- **15:30-16:30 Tipy a triky pro správce eduroamu**
  - Setkání nových správců eduroam, doporučené postupy, individuální konzultace

ODKAZY NA DOKUMENTACI SLUŽEB

- eduid.cz
- eduroam.cz
- pki.cesnet.cz
- tcs.cesnet.cz
- perun-aai.org

- eidas.cesnet.cz (od 1.3.2019)

cesnet

DĚKUJI ZA POZORNOST

MÁTE NĚJAKÉ DOTAZY?