cesnet

DIGITÁLNÍ IDENTITY

Jiří Bořík
CESNET

CESNET Day 23.5.2019
České Budějovice

OBSAH PREZENTACE

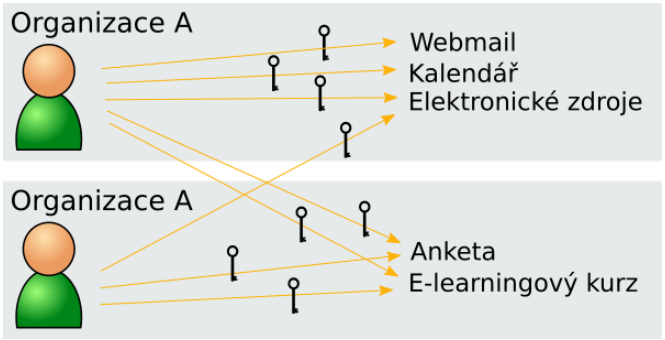
- fyzická a elektronická identita
- federace eduroam
- federace eduID.cz
- elektronické certifikáty
- PKI služby CESNET
- eIDAS
- správa identit a přístupů - Perun

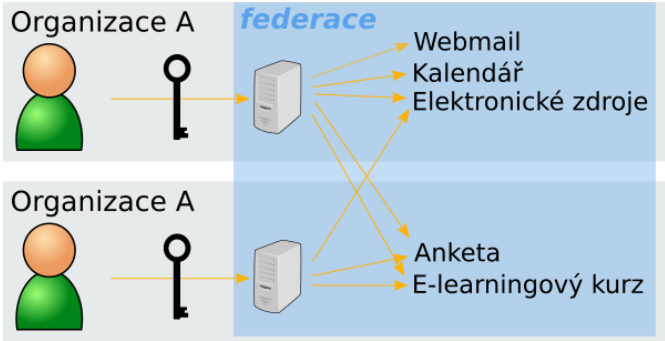
FYZICKÁ A ELEKTRONICKÁ IDENTITA

- **Identita**
  - Fyzická x elektronická
  - Lokální x federovaná
- **Důvěryhodnost - spolehlivé a bezpečné ověření původu**
  - Domovská organizace (statutární orgán, IdP)
  - Nezávislá třetí strana (OP, pas, certifikáty)
- **Ochrana soukromí identity**
  - Zneužití dat identity, podvržení identity
  - Ochrana citlivých dat (nejen osobní data z hlediska GDPR)
  - Bezpečný provoz služby (narušení provozu, dostupnosti…)
- **Snadnost použití identity**
  - 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





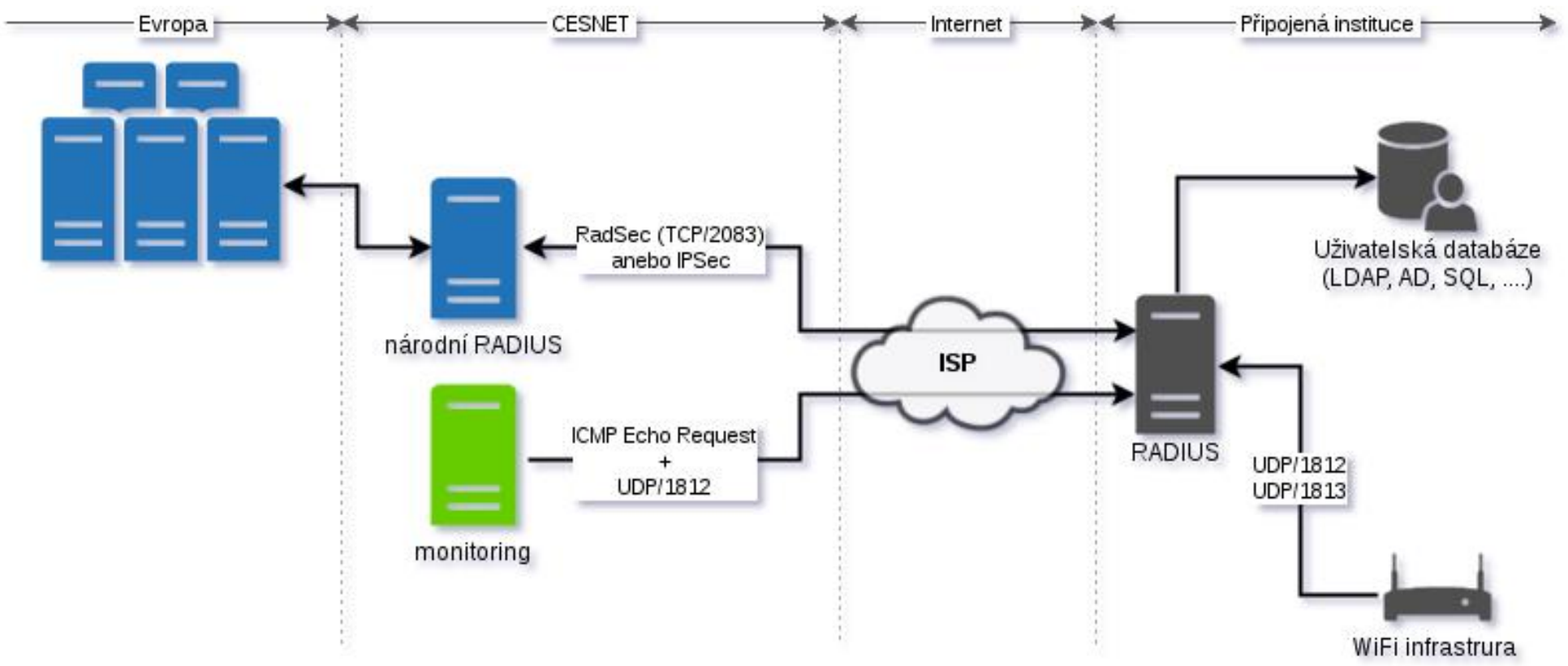
Charakteristika prostředí

- 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

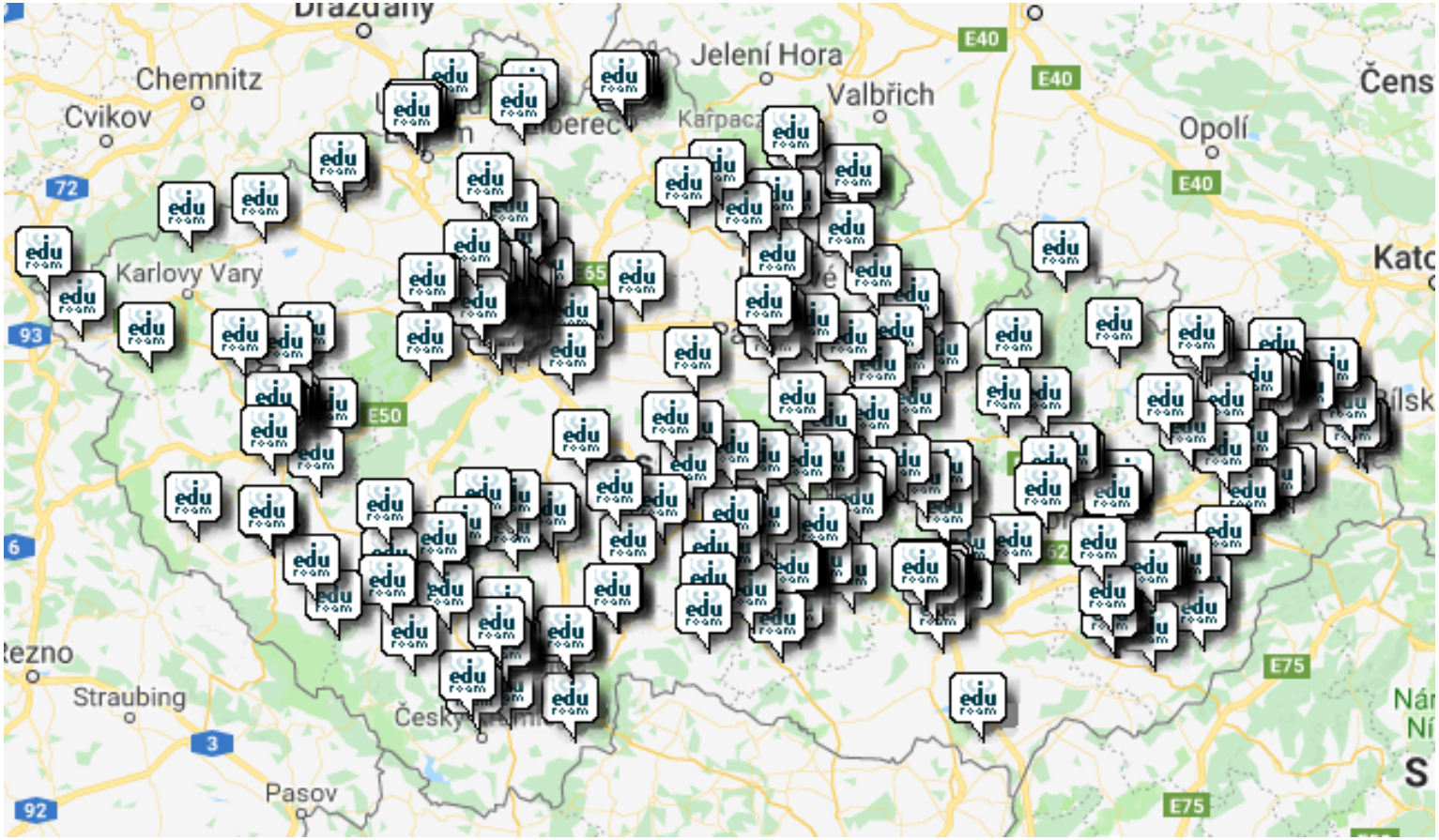
Operátor federace = sdružení CESNET

- 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

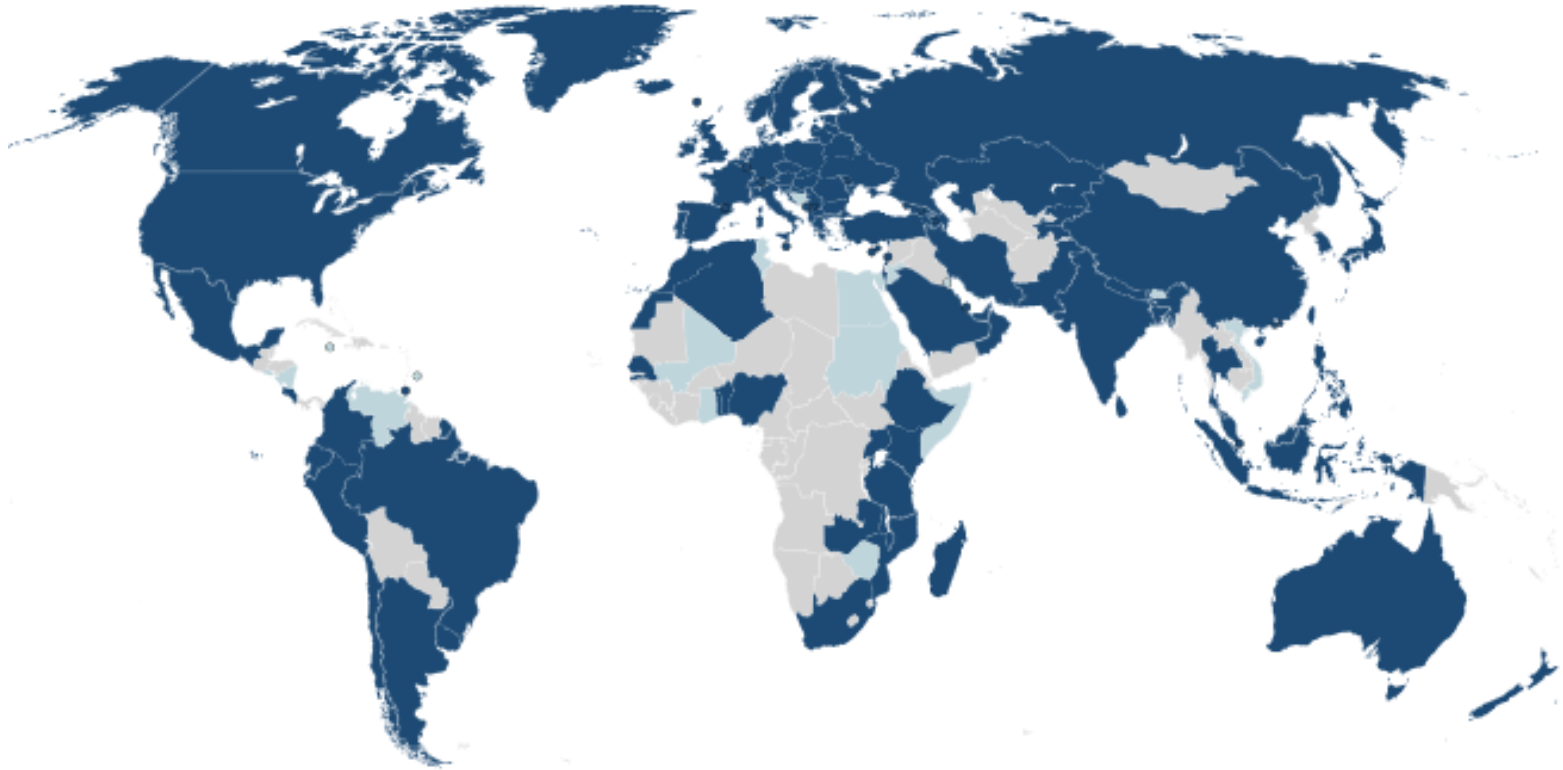


POKRYTÍ ČR


Drážďany
Chemnitz
Cvikov
Jelení Hora
Valbřich
Karpacz
Opolí
Karlovy Vary
Straubing
Pasov
E40
E50
E75
72
93
3
92

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

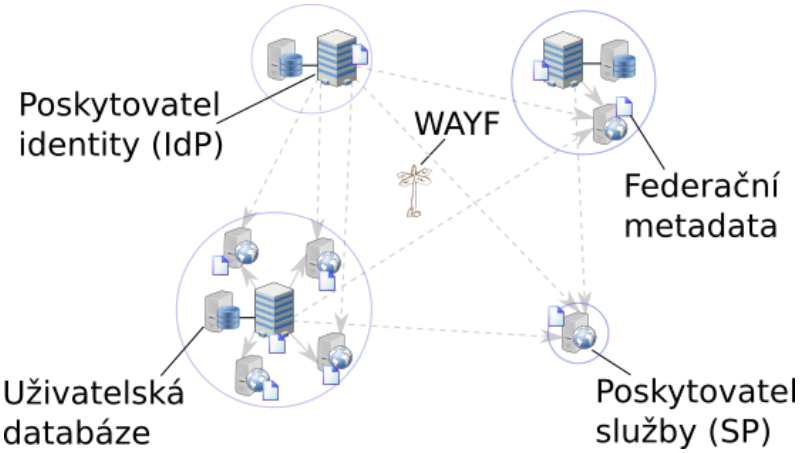
eduID.cz - PRINCIPY

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)

CERTIFIKÁTY

- **Asymetrická kryptografie, veřejný a privátní klíč**
- **Digitální certifikát**
  - Digitálně podepsaný veřejný šifrovací klíč, který vydává certifikační autorita, ve formátu X.509
  - Obsahuje také informace o majiteli veřejného klíče a vydavateli certifikátu (certifikační autoritě)
  - Při vydávání certifikátu probíhá ověření údajů majitele (validace)
    - na různé úrovni, dle typu CA - Selfsign … QCA
- **Webové certifikáty**
  - DV, OV, EV – nejvyšší stupeň důvěry
  - CA v prohlížečích, CA/Browser Forum
- **Osobní podpisové certifikáty**
  - Národní CA akreditované podle eIDAS (v rámci celé Evropy!)
  - Náhrada vlastnoručního podpisu při elektronickém jednání
- **Gridové certifikáty (serverové, osobní)**
  - Vědecká komunita, přístup k výpočetním zdrojům
- **Další oblasti použití certifikátů**
  - Obecně - vydavatel a uživatel sdílí důvěru v ověřeni uživatele certifikátu
  - Serverové, osobní, robotové…

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, projekt Warden a další uživatelské skupiny
  - Přístup přes Web Services, SAML
- **CA není automaticky v prohlížečích a poštovních klientech**

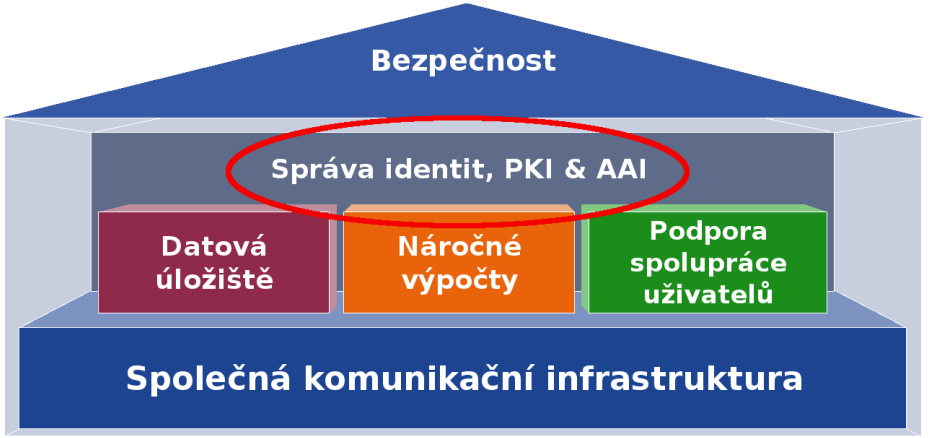
- GÉANT Trusted Certificate Service (TCS)
- Certifikační autorita DigiCert
- Certifikáty s obecně uznávanou platností, např. v prohlížečích
- Vydávané typy certifikátů
  - Serverové (OV, EV)
  - eScience serverové
  - eScience osobní
  - Aplikační (Code Signing)
  - Dokumentové
  - Robotové

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 VVŠ
  - V rámci jejich role Orgánu veřejné moci
- V roce 2019 zahájen společný projekt CESNETu a univerzit
  - Centrální úložiště kvalifikovaných certifikátů
  - Vzdálené podepisování v informačních systémech univerzity
  - Validace podpisů na elektronických dokumentech
  - Související právní analýza
- Aktuální stav
  - Úložiště je v provozu, 2*HSM, umí spravovat certifikáty PostSignum
  - Podpisová aplikace je v provozu proti IS MUNI
  - Připravuje se napojení na další univerzitní systémy

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 (MU, VŠUP)
- Vyhrazená instance součástí projektu eduTEAMS
- Přístup do testovací instance

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

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: '2019-05-22 11:14:00.304'
- USERS: '36068',
- VOS: '331',
- RESOURCES: '2458',
- GROUPS: ‘2146'

ODKAZY NA DOKUMENTACI SLUŽEB

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

cesnet

DĚKUJI ZA POZORNOST