Architektura AAI

Martin Kuba makub@cesnet.cz

Autentizační a Autorizační Infrastruktura

- první potřeba začala se založením MetaCentra (spojená superpočítačová centra UK, MUNI a ZČU) v roce 1996
- uživatelé si volili jméno a heslo pro ssh přístupy na stroje
- ověření identity probíhalo zasláním papírového potvrzení s razítkem domovské instituce uživatele (velmi odrazující)
- vytvořen systém **Perun** pro identity management
  - přijímá přihlášky
  - vytváří a spravuje uživatelské účty na strojích
- v mezinárodním projektu pro fyzikální komunitu DataGrid vznikla v roce 2000 myšlenka výpočetního gridu s autentizací X509 certifikáty

X509 certifikáty a PKI

- uživatel má pár kryptografických klíčů, jeden tajný a druhý veřejný
- založeno na algoritmech RSA (Rivest-Shamir-Adleman, faktorizace velkých prvočísel, 1977) nebo ECC (Elliptic Curve Cryptography,1985)
- certifikát je spojení veřejného klíče s údaji o jeho držiteli, digitálně podepsané certifikační autoritou (CA), formát X509 byl definován v roce 1988
- certifikát CA může být podepsán jinou CA, tvoří řetězce CA
- Public Key Infrastructure (PKI) - infrastruktura správy a distribuce veřejných klíčů
- protokol SSL/TLS z roku 1995 a český zákon č. 227/2000 Sb. o elektronickém podpisu staví na X509/PKI
- uživatel prokazuje totožnost u registrační autority (RA), ta dává pokyn CA k vydání certifikátu

CESNET a Public Key Infrastructure

- CESNET CA vytvořena 28. 6. 2001 ve 13:15:12 GMT
- TEN-155 CZ Server CA pro webové servery také v roce 2001
- v roce 2004 vznikla IGTF - Interoperable Global Trust Federation
- CESNET CA
  - nejdříve offline CA, k serveru se chodilo s disketou
  - pak řešení na HPUX s HSM (Hardware Security Module)
  - současná doba - řešení na Linuxu s HSM
- TCS - TERENA Certificate Service
  - od roku 2010, vystřídali se postupně dodavatelé Comodo, DigiCert, Sectigo (což je bývalé Comodo)
  - self-service vydávání certifikátů, ověření přes SAML federaci
  - od roku 2020 nepoužitelné pro gridové certifikáty

Federace identit a SAML

- v MetaCentru ověřování identity přes papírová potvrzení i X509 certifikáty stále odrazovalo nové uživatele
- v roce 2002 SAML (Security Assertion Markup Language) standardizoval předávání údajů o uživateli od jeho domovské instituce
- v roce 2003 americký projekt Shibboleth vydal software IdP 1.0
- v roce 2005 definován formát SAML v2.0 organizací OASIS
- v roce 2007
  - CESNET založil testovací federaci czTestFed
  - MetaCentrum začalo ověřovat uživatele přes SAML
- v roce 2008 vydán Shibboleth IdP 2.0 s podporou SAML v2.0
- v roce 2009 vznikla ostrá federace eduID.cz, CESNET je operátor

Federace eduID.cz a eduGAIN

- federace je rámec pro vzájemné využívání identit uživatelů při řízení přístupu k síťovým službám
- federace sdružuje organizace, které si chtějí navzájem věřit
- operátor federace vydává seznam zapojených poskytovatelů identit (IdP) a poskytovatelů služeb (SP), a závaznou politiku
- *„česká národní akademická federace identit* ***eduID.cz*** *slouží organizacím zapojeným do sítě CESNET2 při plnění jejich výzkumných a vzdělávacích cílů“*
- **eduGAIN** je celosvětová federace akademických federací používajících SAML, zahrnuje i eduID.cz
- lze autentizovat cca 27 milionů uživatelů eduGAINu

Wi-Fi federace eduroam

- wi-fi federace založená na RADIUS, ne na SAML, jen ano/ne
- začátek v roce 2002 v rámci TERENA mobility TF
- v roce 2003 technicky funkční v ČR
- v roce 2004
  - návrh eduroam politiky
  - propojení s evropskými top level RADIUSy
  - oficiální začátek vysílání essid eduroam na CESNETu
  - připojení prvních členů (fel.cvut.cz, tul.cz, ujep.cz)
- v roce 2005 zapojeno 13 realmů a 13 lokalit v ČR
- v roce 2017 zapojeno 230 realmů a 825 lokalit v ČR, 43 tisíc uživatelů
- v roce 2021 zapojeno 495 realmů a 1121 lokalit v ČR

Mesh a Hub-and-Spoke federace

- eduID.cz je federace typu mesh (síťovina), každý SP si musí vyjednat vydávání dat s každým IdP zvlášť
- nizozemská SURFconext (SURF je nizozemský NREN, obdoba CESNETu) je federace typu hub-and-spoke (náboj a paprsky kola)
- v centru je hub, který směrem k IdP vystupuje jako SP, a směrem k SP jako IdP
- výhoda hub-and-spoke je, že každý IdP a SP vyjednává jen s hubem, ne každý IdP s každým SP, tedy m+n vztahů místo m*n

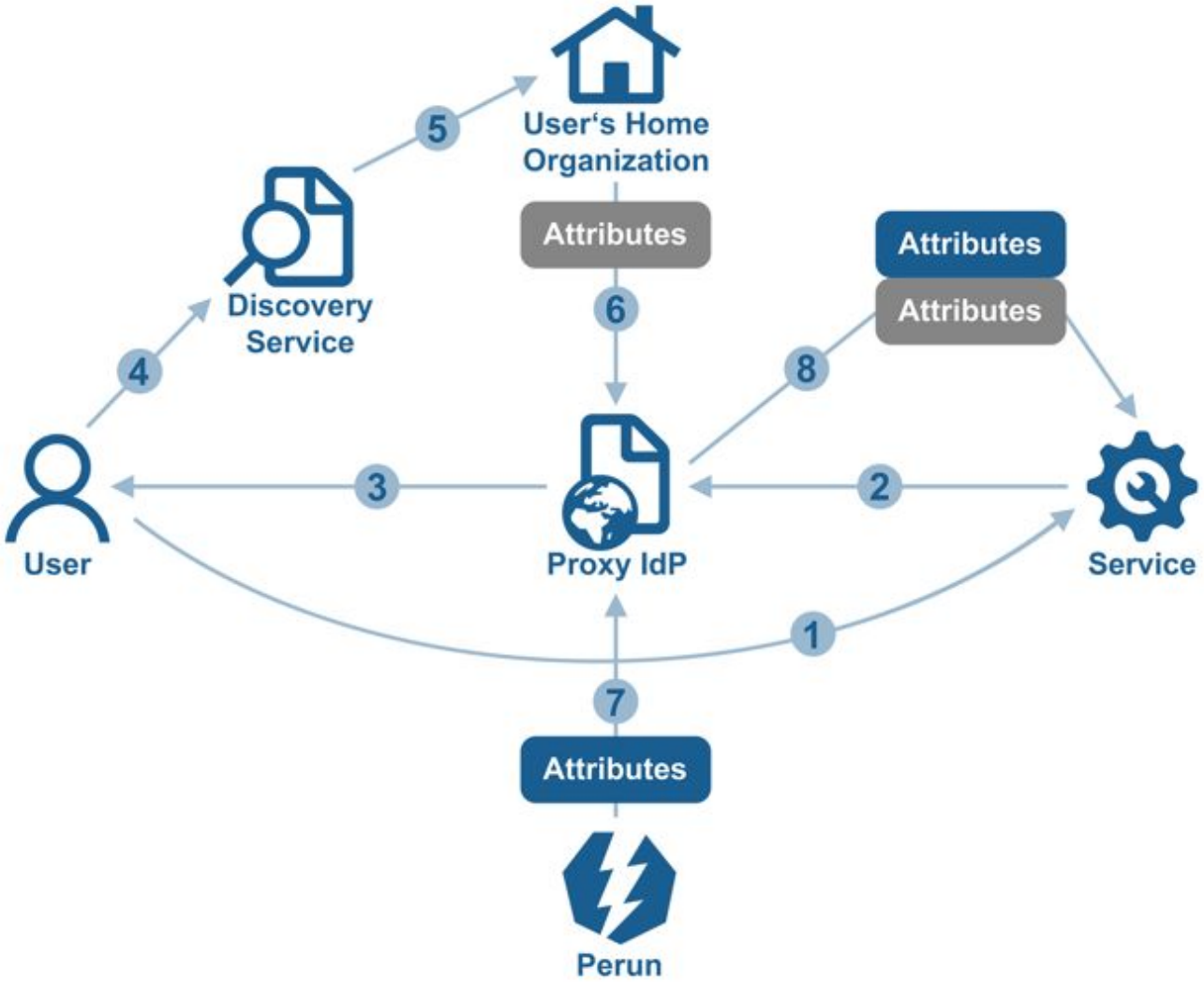
Perun Proxy IdP

- pracovní skupina Perun AAI je společné úsilí CESNETu a MUNI
- pro celoevropskou lifescience infrastrukturu ELIXIR jsme v pracovní skupině Perun AAI vyvinuli tzv. Proxy IdP
- myšlenka je stejná jako hub-and-spoke federace - IdP vůči SP, SP vůči IdP
- navíc je to místo, kde lze držet autorizační informace
  - **autentizace** - ověření identity
  - **autorizace** - proces povolení přístupu
- některé autorizační informace není kde jinde držet, typicky u společných pracovišť nebo projektů mezi více organizacemi
- např. skupina lidí z více institucí s povoleným přístupem k více nástrojům, nelze držet ani na více IdP ani na více SP

Perun AAI

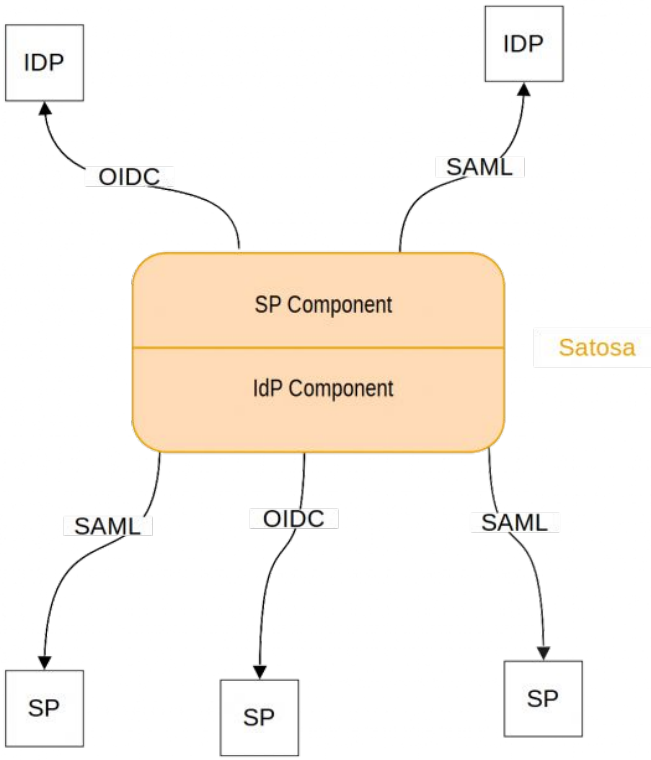
- Perun IdM
  - přijímá přihlášky do virtuálních organizací
  - ověřuje v pravidelných intervalech členství v domovských institucích
  - propojuje různé identity (způsoby autentizace) téže osoby
  - eviduje skupiny a jejich členy, a jejich přístup k prostředkům
  - identity management
    - synchronizuje uživatelské účty z jiných systémů
    - dělá provisioning a deprovisioning uživatelských účtů na spravované výpočetní prostředky
- Proxy IdP napojené na instanci Peruna
  - deleguje autentizaci na domovské IdP
  - přidává dodatečné atributy uživatelům (např. členství ve skupinách v Perunovi, speciální práva v rámci infrastruktury)
  - může udělat autorizační rozhodnutí už před přístupem na SP

Architektura Perun AAI



Implementace Perun AAI

- Proxy IdP
  - směrem k vnějšímu světu
    - protokol SAML do federací - SimpleSamlPhp SP
    - protokoly OAuth nebo OIDC k Google, LinkedIn, GitHub, Apple, ORCID
  - směrem ke službám dvě rozhraní
    - protokol SAML - SimpleSamlPhp IdP
    - protokol OIDC - MITREid
  - spolupracujeme na implementaci SATOSA
  - SATOSA (SamlToSaml) vyvíjí idpy.org
- Perun IdM
  - Core - Java, HTTP API
  - Engine - Java + Perl
  - LDAPconnector - Java + OpenLDAP
  - GUI - Angular a GWT

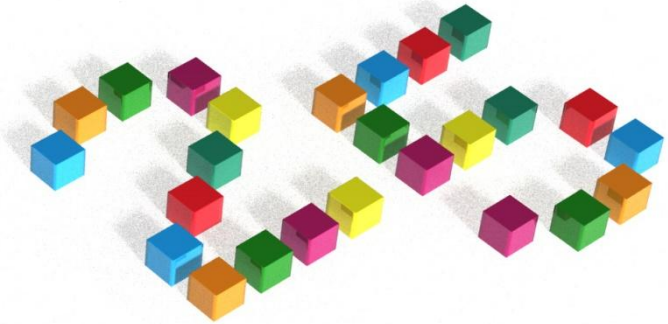


Historie Perun AAI

- Perun v1 pro potřeby MetaCentra v roce 1996 v C+SQL
- Perun v2 s webovým rozhraním v PHP+Perl cca 1998-9
- od 2002 použití X509 certifikátů
- od 2007 připojení na SAML federace
- od 2010 Perun v3 umožňující více VO, reimplementace v Javě
- od 2014 druhá instance Peruna pro MUNI, třetí pro VŠUP 2015
- od 2016 nasazení Perun+ProxyIdP jako ELIXIR AAI
- další instance pro BBMRI a eduTEAMS - Perun+ProxyIdP/SATOSA
- od 2018 ProxyIdP nasazeno pro e-infrastrukturu CESNET, přebírá entityID od SP MetaCentra kvůli vyjednaným dohodám o atributech
- nyní v roce 2021 celkem 13 produkčních instancí Peruna (a dalších 13 ověřovacích), spravováno Ansiblem, CI/CD, Docker kontejnery

Perun AAI nasazeno pro:

- e-infrastruktura CESNET - perun.cesnet.cz, bude perun.e-infra.cz
- Masarykova Univerzita v Brně - perun.muni.cz
- VŠUP v Praze - perun.vsup.cz
- lifescience e-infrastruktura ELIXIR - perun.elixir-czech.cz
- biobanking e-infrastruktura BBMRI - perun.bbmri-eric.eu
- European Lifescience Research Infrastructures - perun.aai.lifescience-ri.eu
- HPC e-infrastruktura FENIX - central-mms.fenix-ri.eu
- UmbrellaId European large neutron and photon facilities - mms.umbrellaid.org
- GÉANT - mms.aai.geant.org
- GÉANT eduTEAMS - mms.eduteams.org
- nizozemský SURF - mms.sram.surf.nl
- ERASMUS - mms.prod.erasmus.eduteams.org
- Evropské HPC projekty - mms.researcher-access.org



Děkuji za pozornost!