Perun

Slávek Licehammer

CESNET

26. 11. 2015

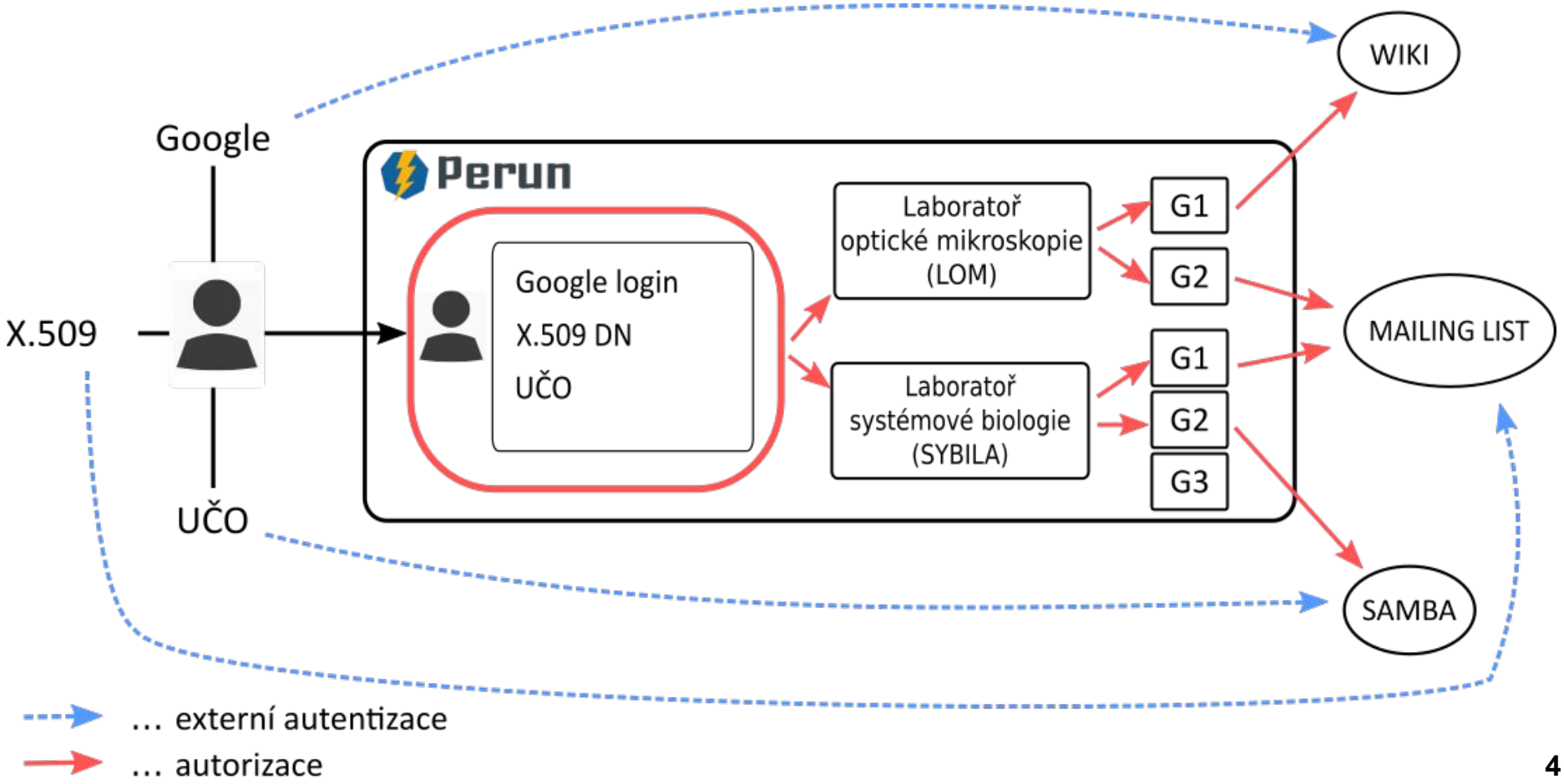
IAM systém

- Nástroj pro centrální správu
  - Uživatelů a jejich identit
  - Skupin
  - Zdrojů
  - Přístupů na služby
  - Registrací
  - Atributů
- Identity and Access Management (IAM) systém

Správa identit

- Podpora různých druhů identit
  - eduID.cz, sociální identity, X.509, …
- Perun zná pouze identifikátory, nikoliv hesla
- Konsolidace identit
  - Prováděná uživateli
- Identity využívány na službách podle potřeb konkrétní služby

Správa identit



Správa služeb

- Není nutné modifikovat služby
  - Perun připravuje autorizační data per služba
  - Data jsou nachystána v požadovaném formátu
  - Transport autorizačních informací je zvolen podle možností služby
  - Podpora standardních protokolů
    - SAML atributová autorita, LDAP, VOOT

Integrace s externími systémy

- Importy uživatelů a skupin
  - umožňuje integraci dalších systémů
  - impozt z SQL, XML, LDAP, VOMS, CSV
  - podpora dynamického mapování
  - možnost pravidelné synchronizace
  - monitoring úspěšnosti synchronizace
  - notifikace

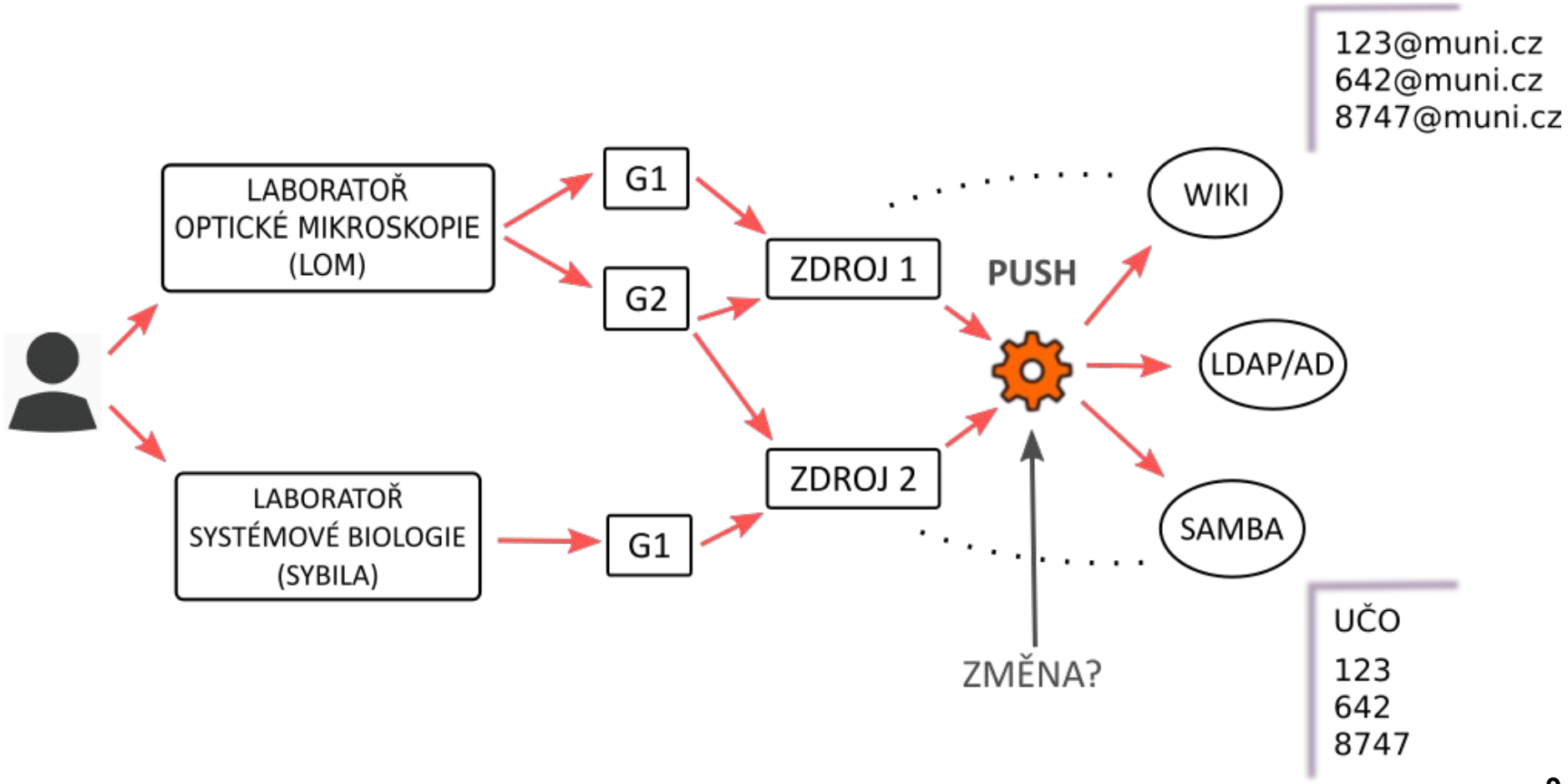
Správa atributů

- Atributy vznikají podle požadavků služeb
- Kontroly syntaxe i sémantiky hodnot
  - včetně vzájemných závislostí
- funkce doTheMagic
  - Automatické generování hodnot
- Napojení na služby a jejich propagace
  - U každé změny v atributu víme, které služby ovlivní

Propagace dat na služby

- Push mechanismus
  - Autorizační data jsou aktivně tlačena na koncové služby
  - Minimalizace single point of failure a odolnost proti síťovým výpadkům
  - Deprovisioning
    - Aktivní suspendování/expirace uživatelů

Push mechanismus

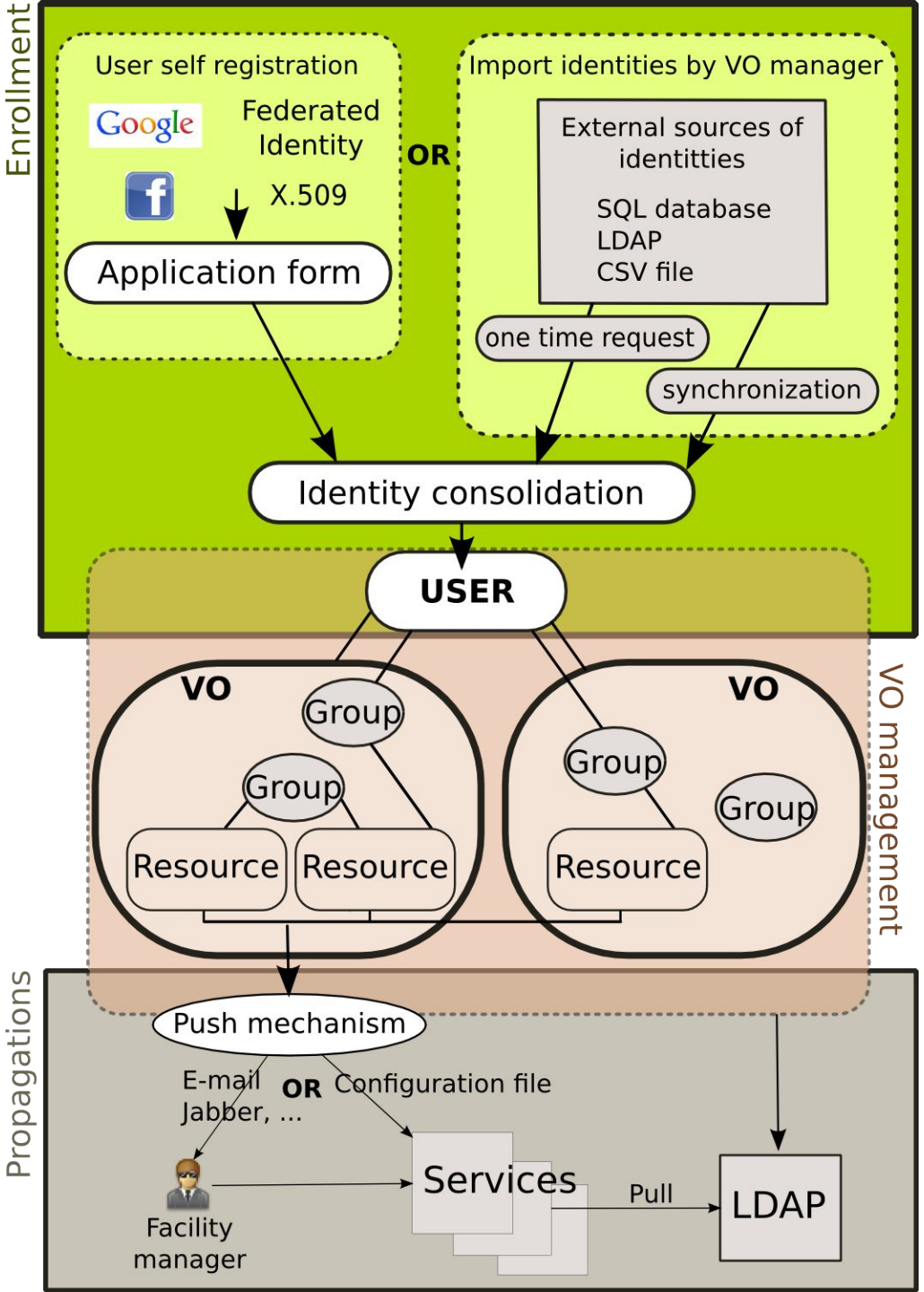


Registrace

- Různé flow pro přihlášky
  - E-mailové pozvánky pro uživatele
  - Self-service
  - Schvalování uživatelů
  - Automatické schvalování po splnění podmínek
- Přihlášky do skupin
- Periodické prodlužování členství
- Podpora přesměrování po vyplnění příhlášky

Klíčové vlastnosti

- Jednotný uživatelský profil
  - Správa záznamů na jednom místě pro všechny služby
- Centrální správa skupin
  - Jedna skupina použitá pro více služeb
  - Možnost synchronizace z externího systému
- Delegování práv
  - Pro správu VO, skupin a služeb


Enrollment
User self registration
Google
Federated Identity
X.509
Application form
OR
Import identities by VO manager
External sources of identitties
SQL database
LDAP
CSV file
one time request
synchronization
Identity consolidation
USER
VO
Group
Group
Resource
Resource
VO
Group
Group
Resource
VO management
Propagations
Push mechanism
E-mail
Jabber, ...
OR
Configuration file
Facility manager
Services
Pull
LDAP

O Perunovi

- Vyvíjený CESNETem a MU
- Open-source
  - https://github.com/CESNET/perun/
- Poskytovaný as a service
  - případně jako virtual appliance
- Nasazení
  - CESNET, MU, EGI, ELIXIR, VŠUP
  - další malé instance

Děkuji za pozornost

http://perun.cesnet.cz
perun@cesnet.cz

Slávek Licehammer
slavek@ics.muni.cz