



Identity and Access Management System
(IAM)

Michal Procházka, Slávek Licehammer
{michalp,slavek}@ics.muni.cz

Co řešíme za problém?



Co řešíme za problém?



přístup uživatelů na služby

Co řešíme za problém?



potřebujeme znát ty **služby**

Co řešíme za problém?



potřebujeme znát i **identitu** uživatelů

Co řešíme za problém?



identity mohou být ale z **různých** zdrojů
(MU, guest)

Co řešíme za problém?



potřebujeme je sdružit do **skupin** pro jednodušší
správu

Co řešíme za problém?



předat tu **správu odpovědným** osobám

Co řešíme za problém?



vhodné řešení je **centrální** s **decentralizovanými**
zdroji dat a správou

Řešení?



Řešení?



Perun jako nástroj pro implementaci globálního
AAI v **existující** organizaci

Globální AAI



Globální AAI



existující digitální identity uživatelů
delegovaná authN

Globální AAI



existující digitální identity uživatelů
delegovaná authN

existující skupiny
delegovaná authZ

Globální AAI



existující digitální identity uživatelů
delegovaná authN

existující skupiny
delegovaná authZ

škálovatelnost

Globální AAI - stereotypy



Globální AAI - stereotypy



rozdělení rolí technický a administrativní správce

Globální AAI - stereotypy



rozdělení rolí technický a administrativní správce

typy skupin: implicitní a explicitní

Globální AAI - stereotypy



rozdělení rolí technický a administrativní správce

typy skupin: implicitní a explicitní

autorizace na základě skupiny/role

Globální AAI - stereotypy



rozdělení rolí technický a administrativní správce

typy skupin: implicitní a explicitní

autorizace na základě skupiny/role

životní cyklus uživatele

Koncept Virtuální organizace



Koncept Virtuální organizace



skupina osob se **společným** zájmem

Koncept Virtuální organizace



skupina osob se **společným** zájmem

+

mající **správce**

Koncept Virtuální organizace



skupina osob se **společným** zájmem

+

mající **správce**

+

a definovanými **pravidly** pro členství

Virtuální organizace - Vlastnosti



Virtuální organizace - Vlastnosti



osoba má role ve VO

Virtuální organizace - Vlastnosti



osoba má role ve VO

členové mohou být vnitřně organizováni do skupin

Virtuální organizace - Vlastnosti



osoba má role ve VO

členové mohou být vnitřně organizováni do skupin

proti běžné skupině má k dispozici zdroje

Virtuální organizace - Vlastnosti



osoba má role ve VO

členové mohou být vnitřně organizováni do skupin

proti běžné skupině má k dispozici zdroje,
ke kterým se definuje přístup svých členů

Uživatel v Perunovi



Uživatel v Perunovi



každý z nás má **několik** digitálních identit

Uživatel v Perunovi



každý z nás má několik digitálních identit

nechceme zavádět další

Uživatel v Perunovi



každý z nás má několik digitálních identit

nechceme zavádět další

vazba osoba <-> uživatel v Perunovi

Uživatel v Perunovi



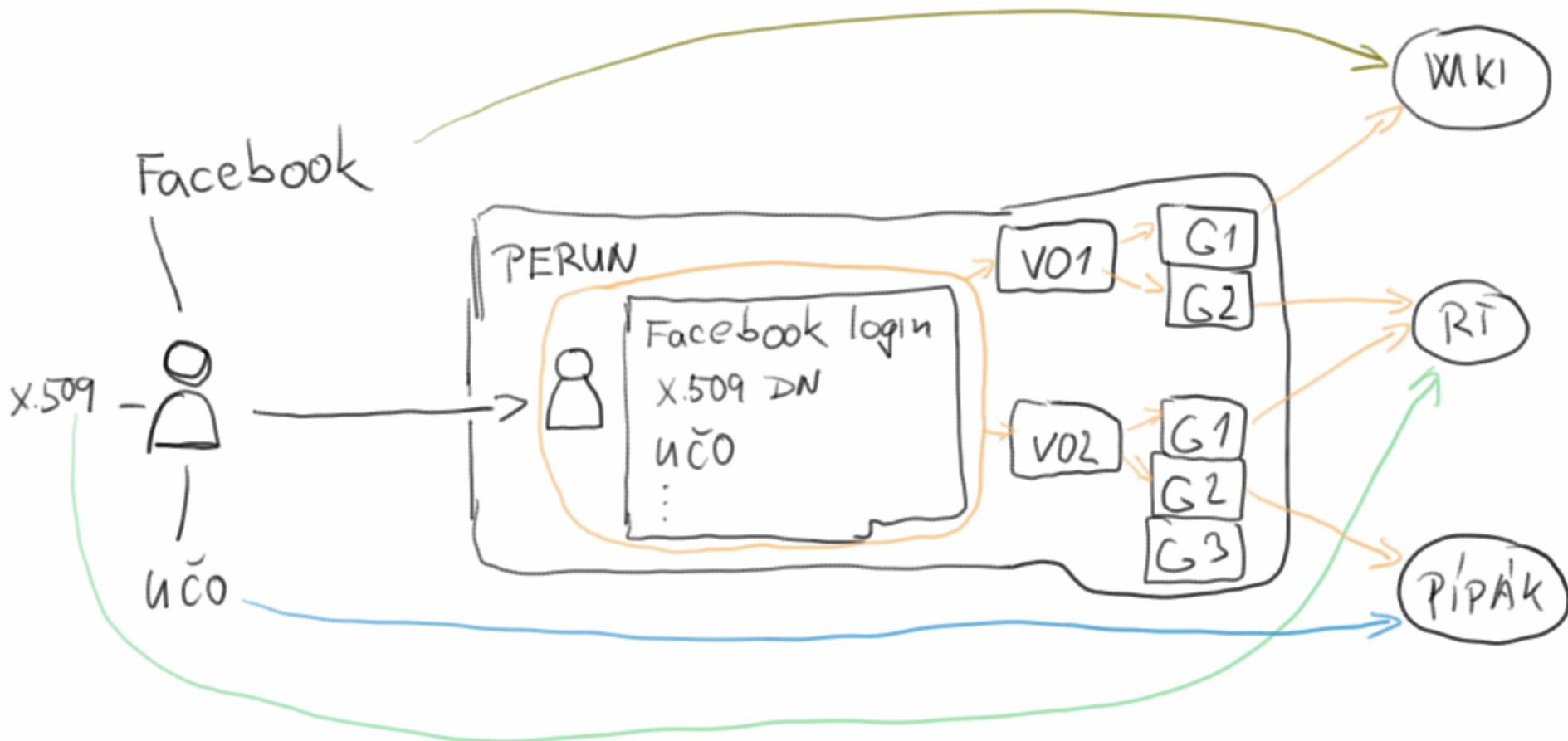
každý z nás má několik digitálních identit

nechceme zavádět další

vazba osoba <-> uživatel v Perunovi

doba trvanlivosti uživatele

Uživatel v Perunovi



Delegování rolí



Delegování rolí



delegovat správu uživatelů a zdrojů na **odpovědné**
osoby

Delegování rolí



delegovat správu uživatelů a zdrojů na odpovědné osoby

technický vs. administrativní správce zdroje (např. přístup na přípáky)

Správa zdrojů



Správa zdrojů



řízení **přístupu** na zdroje **administrativní** osobou

Správa zdrojů



řízení **přístupu** na zdroje **administrativní** osobou
správa **nastavení** služby **technickou** osobou

Správa zdrojů



řízení **přístupu** na zdroje **administrativní** osobou

správa **nastavení** služby **technickou** osobou



nutnost evidence zdrojů

Správa zdrojů



řízení přístupu na zdroje administrativní osobou

správa nastavení služby technickou osobou



nutnost evidence zdrojů

evidence vazby uživatel-skupina-zdroj => authZ

Správa zdrojů



řízení přístupu na zdroje administrativní osobou

správa nastavení služby technickou osobou

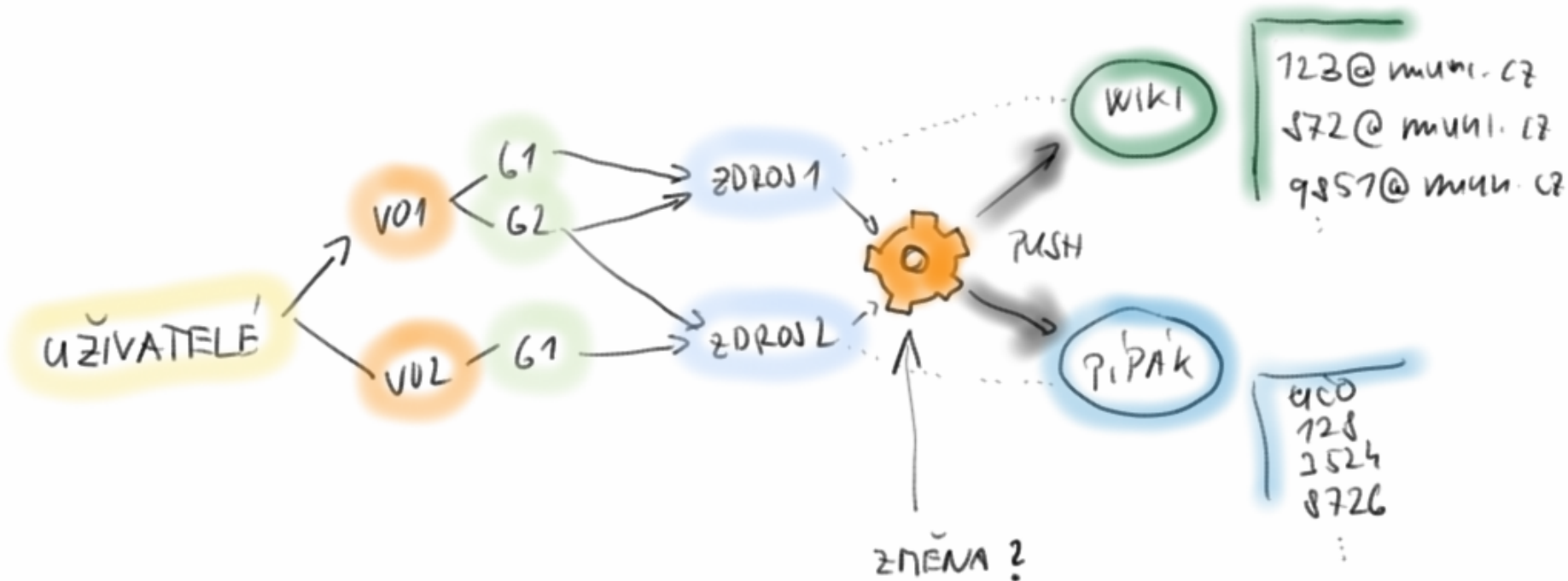


nutnost evidence zdrojů

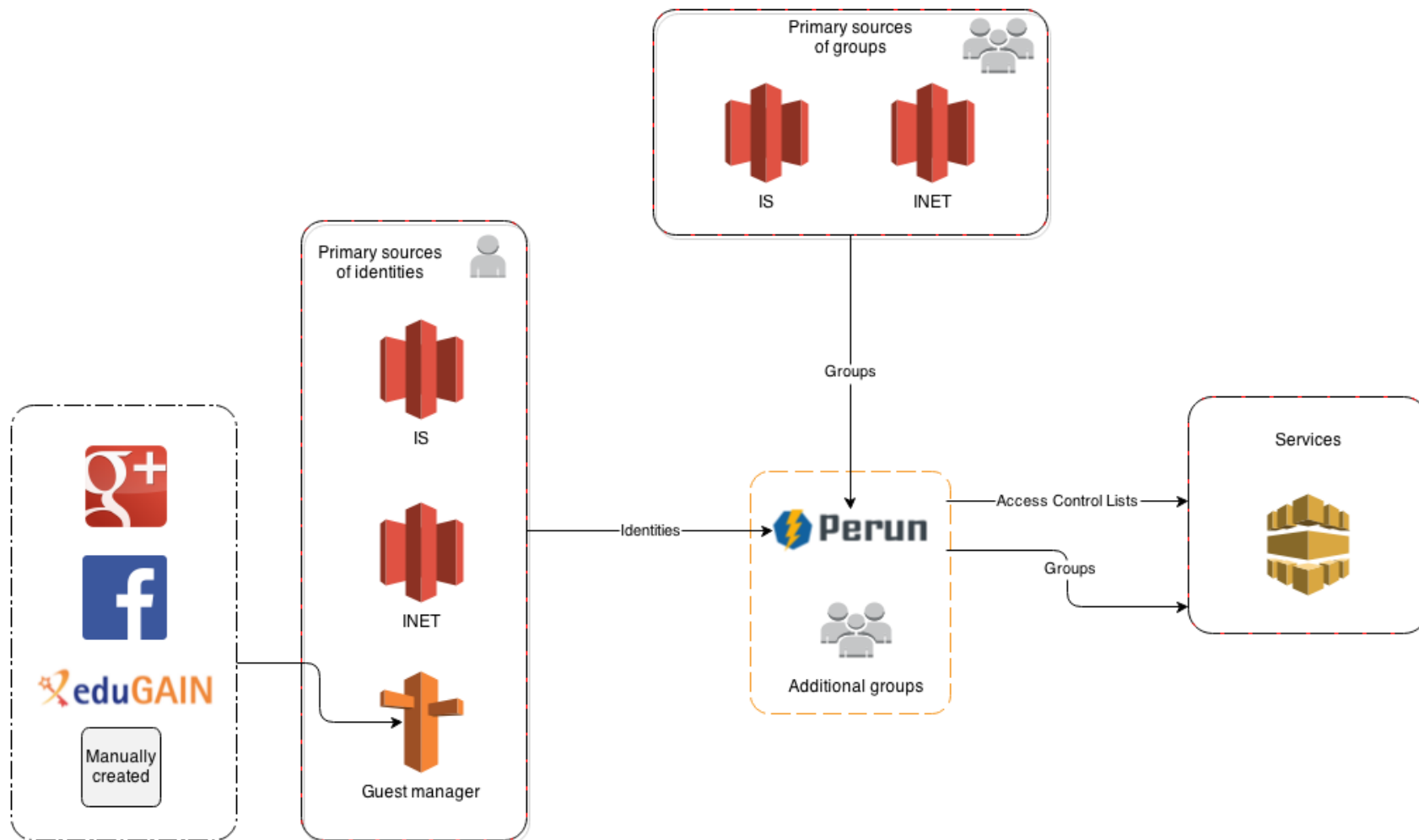
evidence vazby uživatel-skupina-zdroj => authZ

propagace přístupových práv na zdroje

Správa zdrojů



Role Peruna na MU



Vývoj Peruna



Vývoj Peruna



12 lidí v týmu

Vývoj Peruna



12 lidí v týmu
zaučování studentů

Vývoj Peruna



12 lidí v týmu

zaučování studentů

řízený vývoj a nasazování

Vývoj Peruna



12 lidí v týmu

zaučování studentů

řízený vývoj a nasazování

open source + GitHub

Vývoj Peruna



12 lidí v týmu

zaučování studentů

řízený vývoj a nasazování

open source + GitHub

použité technologie

Java, Spring, GWT, JavaDoc, Bash, Perl

Maven, Jenkins

Git

Statistiky / CESNETí instance



Statistiky / CESNETí instance



23 měsíců v provozu

Statistiky / CESNETí instance



23 měsíců v provozu

164 virtuálních organizací

Statistiky / CESNETí instance



23 měsíců v provozu

164 virtuálních organizací

4208 uživatelů

Statistiky / CESNETí instance



23 měsíců v provozu

164 virtuálních organizací

4208 uživatelů

716 skupin

Statistiky / CESNETí instance



23 měsíců v provozu

164 virtuálních organizací

4208 uživatelů

716 skupin

1808 spravovaných zdrojů

Vybrané funkce Peruna



- ukázka GUI
- práce s přihláškami
- práce se skupinami
- ukázka mini aplikace
- ukázka zdrojů
- ukázka propagace dat na zdroje



<http://perun.cesnet.cz>

perun@cesnet.cz