Systém pro řízení přístupu ke službám

Michal Procházka

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007–13
OP Výzkum a vývoj pro inovace

Perun

O čem to celé bude?

- O systému pro správu uživatelů, skupin a řízení přístupu na služby
- O jeho využití jako služby pro Vaše potřeby

Motivace

- V rámci e-Infrastruktury CESNET je mnoho služeb určených pro koncové uživatele
- Služby vyžadují prokázání identity uživatele (autentizaci)
- Uživatel chce přistupovat ke službám komfortně
  - Analogie Google účtu

Perun

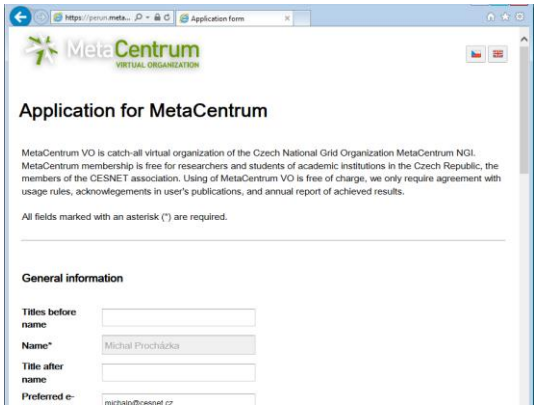
Co k tomu potřebujeme?

- Jednotnou identitu uživatele
- Správa uživatelských údajů na jednom místě

- Rozhraní pro konfiguraci kdo kam může
- Evidenci služeb

Jak to dělá CESNET?

- Přístup k MetaCentru a CESNET DÚ je řízen centrálně
  - Vytváření uživatelských účtů
  - Řízení mailing listů
  - Přístup k licencím software
  - Řízení kvót na uložištích
- Jednotný účet uživatele v e-Infrastruktuře s definovaným životním cyklem



Perun **Účet v e-Infrastruktuře**

Služby e-Infrastruktury

- Datová uložiště
- SIP
- CERTS
- Anti-SPAM
- IP Tel.

- Systém pro správu uživatelů a skupin
  - Organizování uživatelů do nezávislých celků
    - Virtuální organizace = skupina uživatelů se správci a definovanými pravidly pro členství
  - Delegování správy skupin na odpovědné osoby

- Systém pro řízení přístupu ke službám
  - Evidence služeb
  - Řízení která skupina může na kterou službu a za jakých podmínek

Delegování odpovědnosti

- Správci služeb definují kterým VO bude služba dostupná a za jakých podmínek
- Správce VO řídí členství ve VO
- Správce VO určuje, kdo z členů VO může danou službu využívat a nebo toto právo deleguje

Konfigurace přístupu na služby

- Exportuje seznam povolených členů na službu
  - Přímo konfiguruje služby
  - Vystavuje v požadovaném formátu
- Správce služby má plnou kontrolu nad procesem konfigurace

A co s tím?

- **Oddělení správy služeb od správy uživatelů služeb**
- Odstranění administrativních a technických překážek při registraci uživatele k službě
- SaaS – minimalizace nákladů na správu

Příklad z praxe

- Chceme pro členy projektu přístup na wiki, interní webové stránky projektu a mailing list
- Členové projektu jsou z různých organizací (akademických i komerčních)
- Předpokládá se fluktuace členů
- **Nechceme dedikovat administrátora na řešení tohoto problému**

Příklad z praxe

- Přístup členů přes eduID.cz/Hostel
- Členství a přístup na služby spravuje manažer projektu (**nikoliv** administrátor služeb)
- Podpora delegace pravomocí manažerem na členy projektu
- Vývojový tým Peruna je řízen tímto způsobem

Závěrem

- Pro zájemce uspořádáme detailní prezentaci
- Pomůžeme s testováním využití Peruna na Vaši instituci
- V současné době systém Perun spravuje cca 2500 uživatelů a 1600 strojů

http://perun.cesnet.cz

perun@cesnet.cz

Michal Procházka