

Federace identit: Úvod do problematiky

- **Authentizace:** správa účtů (identita, ověřovací údaje)
- **Authorizace:** přístup pro daného uživatele k dané operaci v dané službě (v čase)
- AA federovaná, AA federovaná + lokální atributy
- **Security Assertion Markup Language (SAML)** – definice datových formátů a síťových protokolů
- **Identity Provider (IdP):** správa identit, správa ověřovacích údajů, správa atributů
- **Atributová autorita (AA):** spravuje atributy
- **Service provider (SP):** konzumuje potvrzení od IdP a AA
- **Metadata – zdroj důvěry**

EntityDescriptor – datová struktura popisující Entitu

- Role (SP, IdP, AA ...)
- Umístění (URL)
- Parametry služeb (vyžadované atributy..., poskytované formáty dat ...)
- Veřejné klíče

Podepsaného důvěryhodným zdrojem (metadata publisher)

Federace identit

- společenství navzájem si důvěřujících poskytovatelů identit a poskytovatelů služeb.
 - o shodná pravidla:
 - kvalita identit
 - dostupnost a významnost atributů
 - definovaná odpovědnost vzhledem k ochraně soukromí

Operátor federace

- registrace členů
- správa metadat
- dodržování pravidel:
 - o politika federace
 - o technické podmínky
- vztahy s okolními federacemi (česká federace: edu ID cz)

Jak funguje Service Provider – ukázka (Jan Tomášek)

JFSP:

- Architektura
- Atributy: (Affiliation, authorisedMail, cn, entitlement, eppn, givenName, isMemberOf, mail, orgName, sn, tcsPersonalID, remote: ADDR atd.)

<http://www.eduid.cz/wiki/eduid/admins/howto/deploy/index>

Jak funguje IdP

- nad databází uživatelů funguje jako rozhraní
- zabezpečuje session po určitou dobu, které zabezpečuje přístupování k dalším aplikacím bez nutnosti opětovného přihlašování pomocí přihlašovací údajů.

Implementace:

- Shibboleth
- simpleSAMLphp
- Jiné SAML – kompatibilní implementace
- Kompatibilita

Co je potřeba k provozu IdP?:

- databáze uživatelů
- napojení IdP na existující správu uživatelů
- LDAP jako nejběžnější rozhraní pro uživatelskou databázi
- Možnost konverze zdrojových dat na úrovni IdP

Authentizace:

- modulární implementace autentizace
- standartní autentizační moduly: (username-password, jiné)
- možnost implementace vlastních autentizačních modulů

Atributy:

- zdroje uživatelských atributů: LDAP, SQL databáze, statické atributy
- konverze a transformace atributů
- řízené uvolňování atributů

Bezpečnost:

- z hlediska uživatele
- ochrana osobních údajů:
 - o autentizační údaje se přenáší pouze mezi uživatelem a jeho domovským IdP
 - o utajená identita uživatelů
 - o omezení vydávaných atributů – SP dostávají pouze nezbytná data

Česká federace identit = eduID.cz