MASARYKOVA UNIVERZITA
INSTITUT BIOSTATISTIKY A ANALÝZ

Federativní autentizační metody

Martin Komenda

Single Sign-On (SSO)

- Uživatel používá pouze jednotné přihlašovací jméno a heslo pro přístup k více aplikacím

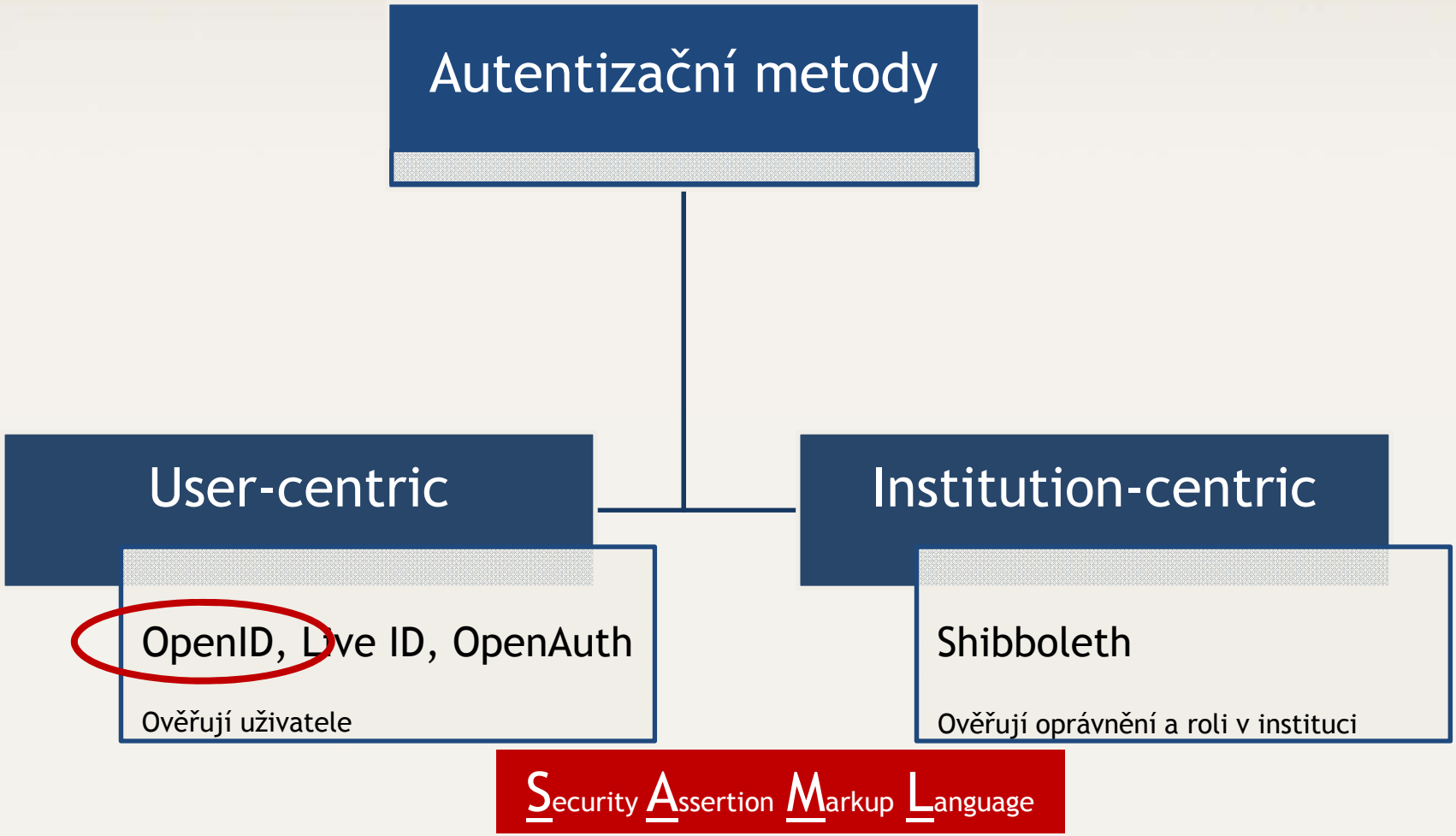
- Výhody
  - + Zvýšení zabezpečení přístupů
    - Eliminace udržování mnoha příhlašovacích údajů (zapomenutí a obnova)
    - Zamezení zneužití snadných hesel
  - + Zvýšení efektivity práce uživatelů a zamezení neustálému přihlašování do jednotlivých aplikací
  - + Bezpečnostní standardy vynucují používání silných hesel (obtížně zapamatovatelná)

- Nevýhody
  - - Pří vyzrazení údajů ohrožen přístup ke všem službám

Single Sign-On (SSO)

- Správci jednotlivých aplikací (SP) neshromažďují přístupové údaje
  - Poskytují uživatelům federace pouze online služby a zdroje
- Autentizace uživatele probíhá na straně poskytovatele identit (IdP)
  - Napojené na uživatelské databáze, provádí autentizaci a poskytují informace o uživatelích

Základní dělení



User-centric autentizace

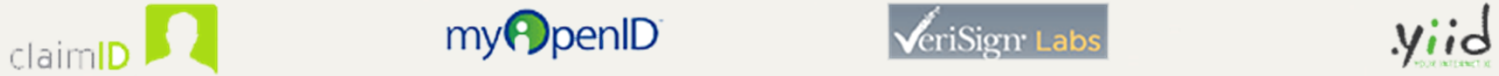
- Přístupové údaje lze využít pro přihlašování také na jiných službách

- Možnosti
  - Uživatel si může vybrat důvěryhodný subjekt
    - OpenID 
  - Důvěryhodný subjekt je pevně daný
    - Live ID, OpenAuth

OpenID

- Uživatel má založen účet u důvěryhodné služby
  - AOL, BBC, Google, IBM, MySpace, Orange, PayPal, VeriSign, LiveJournal, Yandex, Ustream, Yahoo, Seznam, …

  - Další poskytovatele identit (free and secure OpenID)



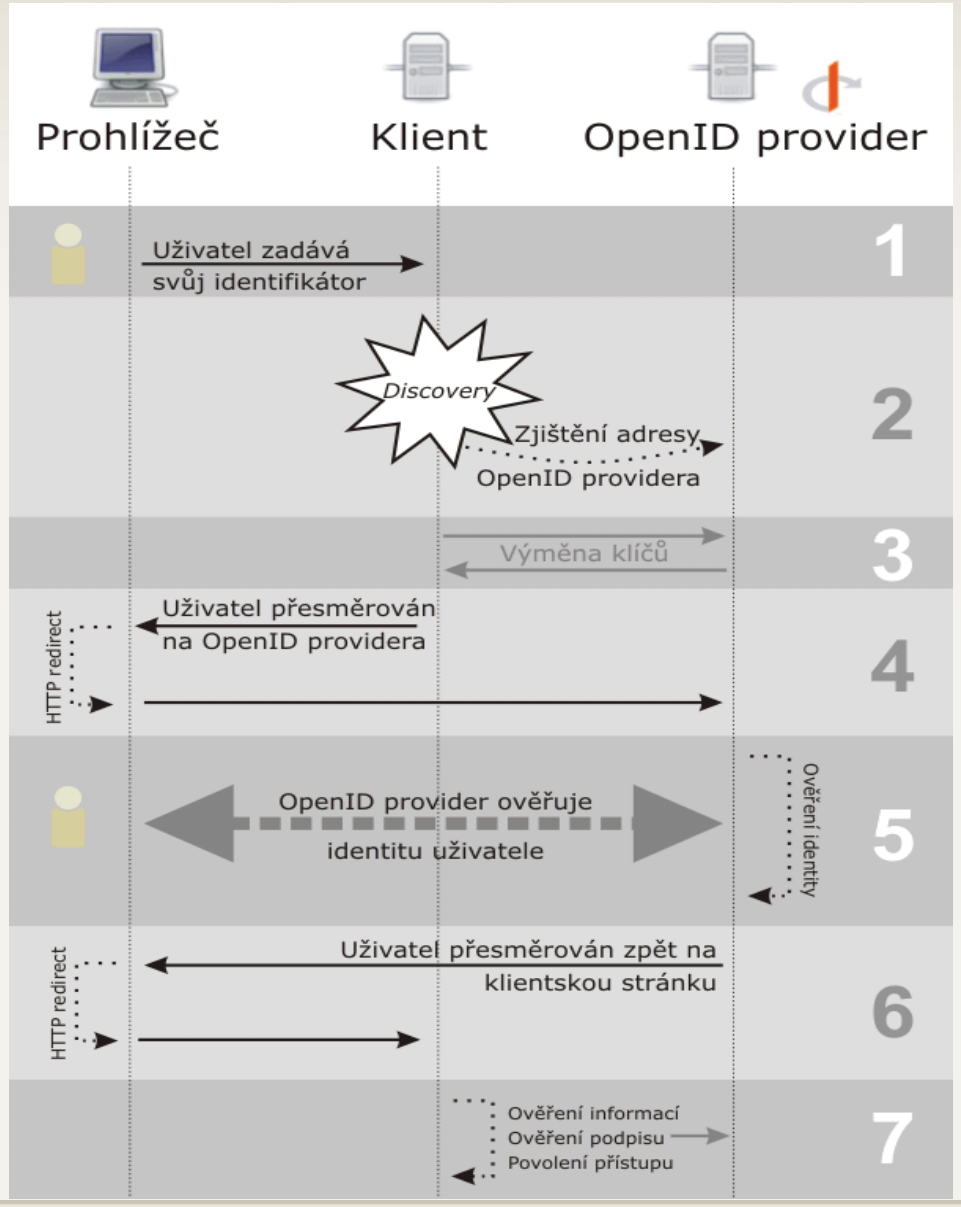
OpenID

- Otevřený standard popisující autentizaci uživatele
- Poskytovatel služby (SP) nemusí zajišťovat autentizaci
- Uživatel se může rozhodnout, komu své údaje svěří
- Princip přesměrování požadavku na ověření identity na poskytovatele OpenID účtu
  - ➡ ten vrátí informaci o výsledku autentizace

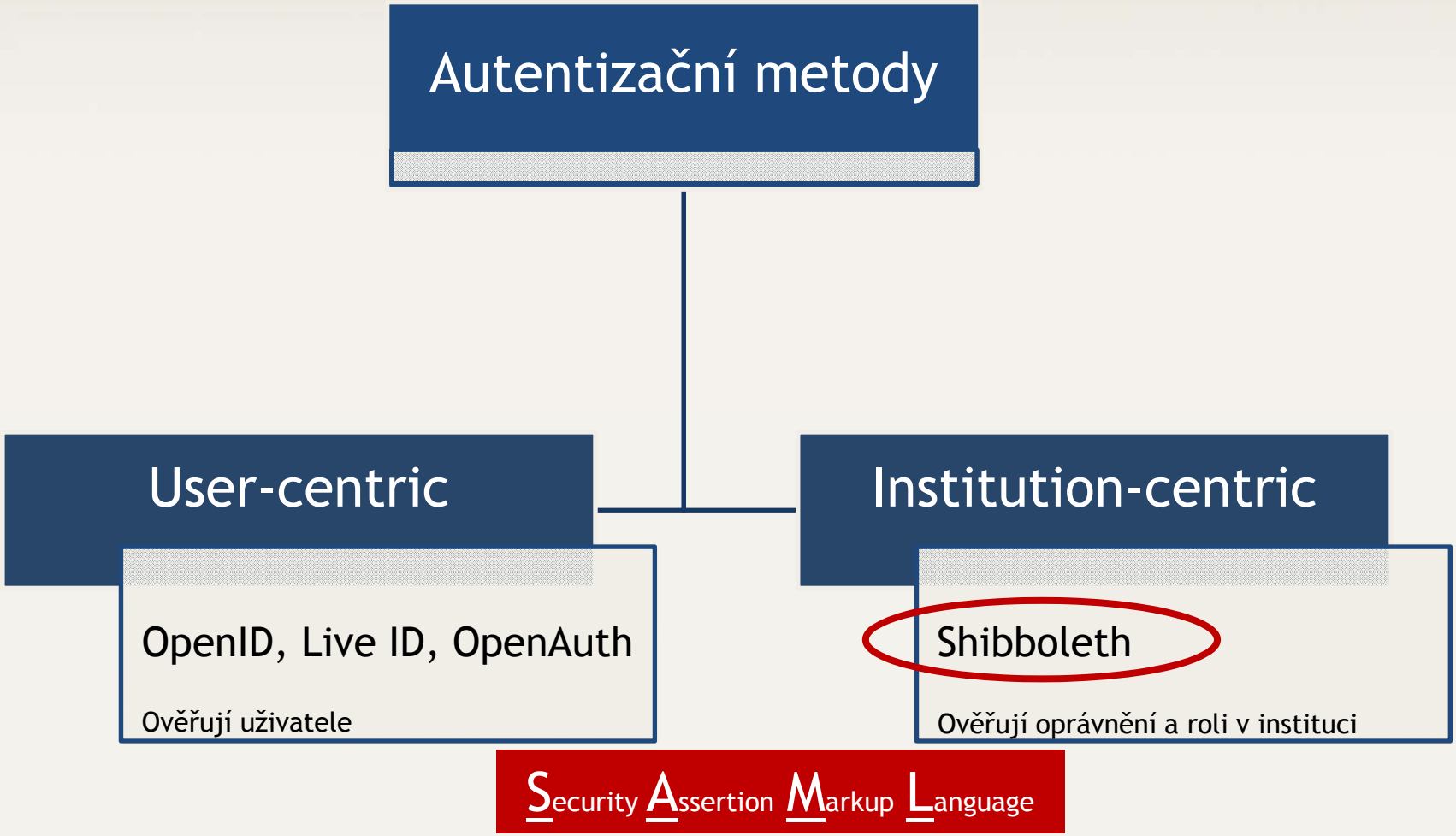
OpenID

- Standard neurčuje, jak je ověření identity realizováno
  - Jméno/heslo, SMS kód, e-klíč, biometrika
    - Zajištěno na straně poskytovatele OpenID
- Jak získat OpenID
  - Get an OpenID: http://openid.net/get-an-openid/

OpenID - proces ověření



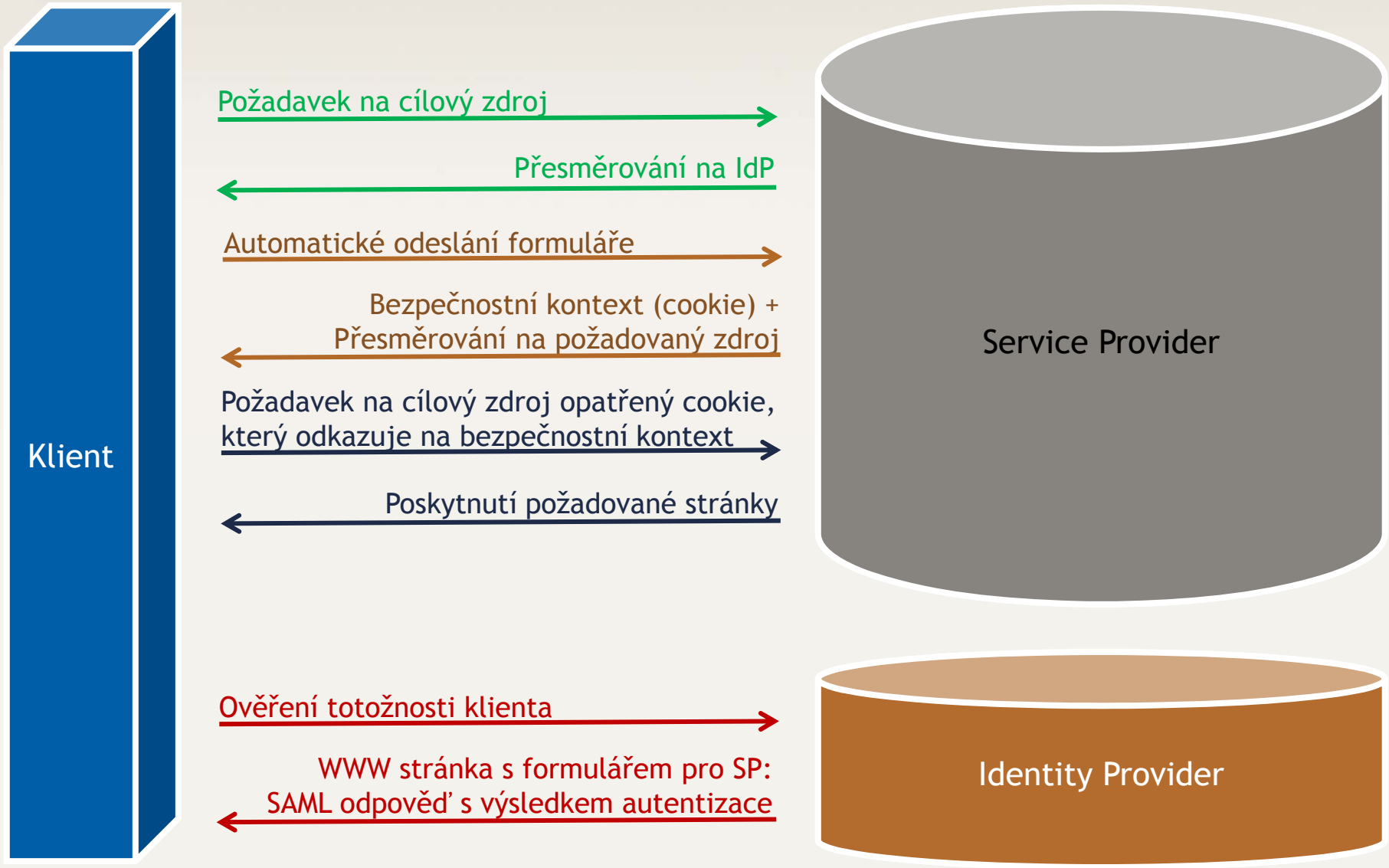
Základní dělení



Institution-centric autentizace

- Uživatel může použít institucionální údaje pro přístup k dalším službám
- Autentizace uživatele probíhá u domovské instituce
- Úrovně přístupu může řídit jak domovská instituce, tak i poskytovatel služby
- Poskytovatel identit v rámci ČR = eduID.cz
- Technologie Shibboleth
  - poskytuje nástroje pro implementaci SSO

Shibboleth - proces ověření



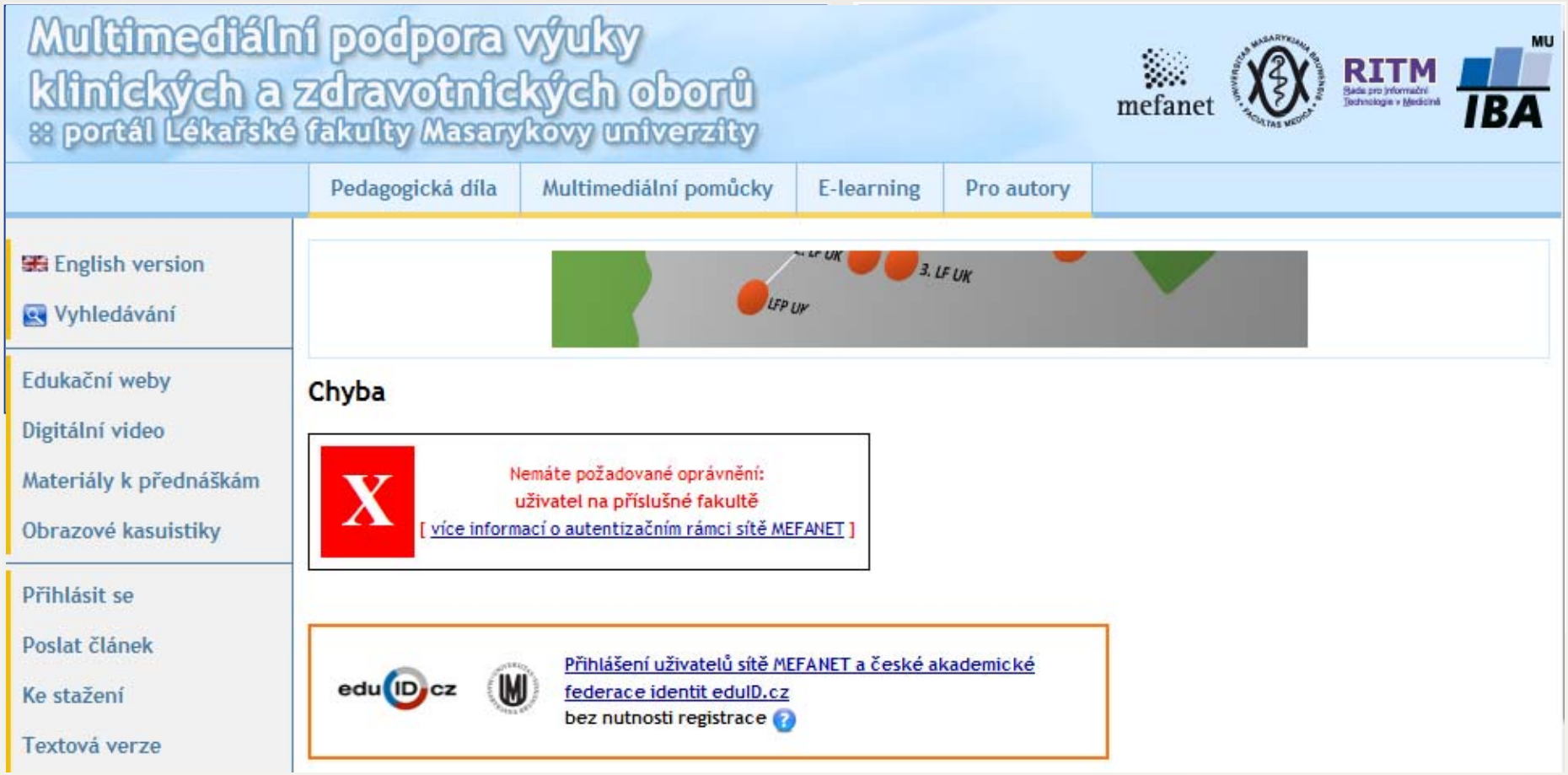
Institution-centric autentizace

- SAML odpověď v podstatě jen říká

  „potvrzujeme, že je to náš uživatel“

- SP nemusí vědět, odkud uživatel pochází a na kterého poskytovatele identit se tudíž obrátit.
  - WAYF (Where Are You From)
    - Formulář s nabídkou spolupracujících institucí a uživatel si sám vybere odkud je.

Institution-centric autentizace: ukázka



Institution-centric: Porovnání

- Ve světě mimo instituce ztrácí svou zásadní výhodu
  - Těžkopádná autentizační metoda s mnoha nevýhodami
  - Po ukončení členství je uživatel mimo hru
- U Shibbolethu platí, že domovská organizace dodává poskytovatelům webových služeb garantované informace o uživatelích
- Poskytovatel na základě licenčních smluv mezi organizací a poskytovatelem nabízí dané služby

SAML

- Security Assertion Markup Language
- Standard pro výměnu dat mezi IdP a SP založený na XML
- Řeší problém jednotného přihlašování na více webů - Single Sign-On (SSO)
- Poskytuje distribuci ověřovacích informací, nespecifikuje implementaci ověřovacích mechanismů na straně IdP

1. Uživatel chce přistupovat ke zdrojům SP
2. Identita uživatele je validována jeho IdP
3. IdP posílá informaci o ověření uživatele SP
   = odpovědnost přesunuta na IdP

SAML

- Nejčastěji se používá ve standardu OpenID nebo u technologie Shibboleth
- Zvyšuje bezpečnost
  - Minimalizuje zadávání přihlašovacích údajů
  - Uživatel uchovává jeden login a heslo
- Zjednodušuje přístup k webovým službám
  - Jednou proběhne autentizace a poté mohu využívat různé služby
- Zjednodušuje správu hesel a administrativu s tím spojenou

SAMP - jak pracuje

Má učet

Chce využít službu

Přistupuje ke službě

Identity Provider

Organizace spravující uživatele a jejich autetizaci

Probíhá ověření identity uživatele

new session

Service Provider

Organizace poskytující webovou službu

Více informací: dokument Autentizační metody

Obsah

- Terminologie
- Autentizační metody
- User-centric autentizace
- Institution-centric autentizace
- Zdroje