

STORK

Secure Identity Across Borders Linked

Michal Procházka

CESNET

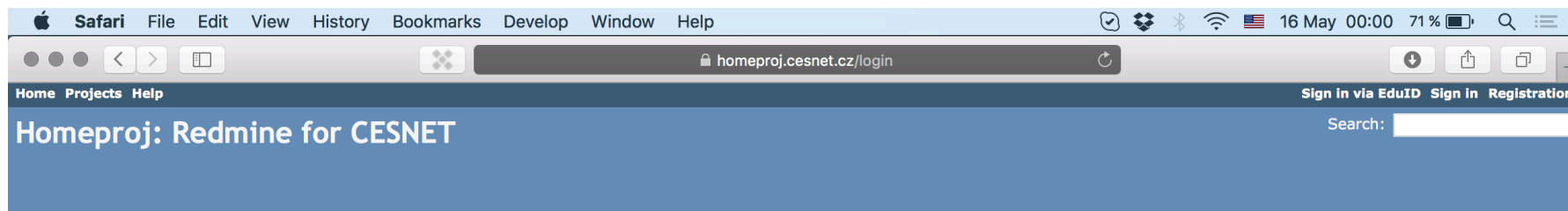
Ústav výpočetní techniky - Masarykova univerzita

EurOpen 2016 – Jindřichův Hradec

Obsah

- Autentizace
- Single Sign-On
- Federované přihlášení
- Federace identit
- STORK
- STORK2
- eIDAS
- eID a ČR

Autentizace



Login:

Password:

Login »

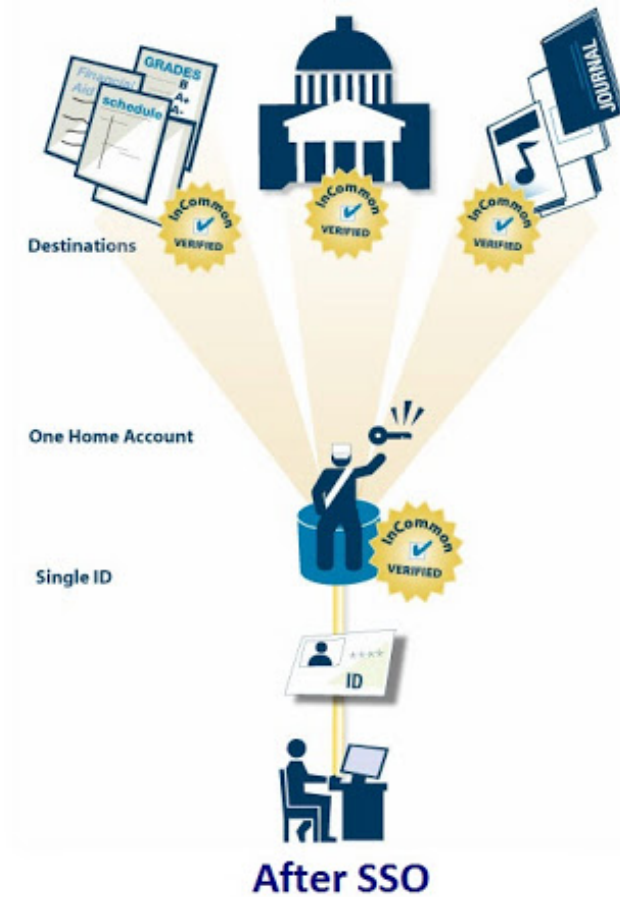
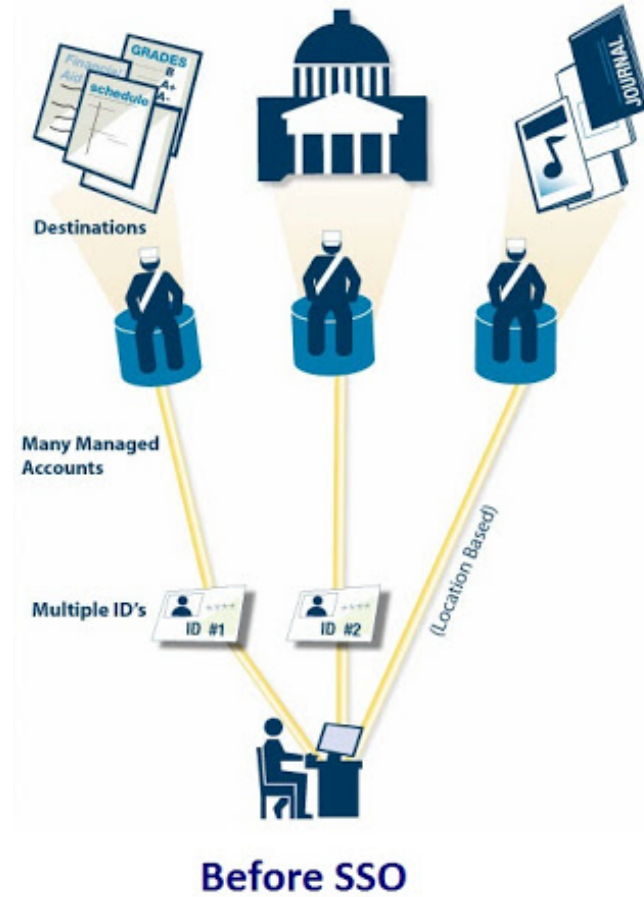
Autentizace

- Přihlášení ke službě – identifikace uživatele
- Každý uživatel má své přihlašovací údaje
- Existují dvojice **uživatel-slужba**
 - Exploze přihlašovacích údajů

Single Sign-On

- Minimalizace počtu vazeb **uživatel-slужba**
- Zavádění v organizacích
 - Minimální dopad na služby mimo organizaci
- Globální Single Sign-On předpokládá unifikovanou technologii a globální důvěru

Single Sign-On



Poskytovatelé sociálních služeb

- Kandidáti na "globální" Single Sign-On
 - Předpokládá, že všichni u nich máme účet
- Využití přihlašovacích údajů poskytovatelů sociálních služeb
- Uzavřený eco-systém
- Neexistující důvěra v identitu

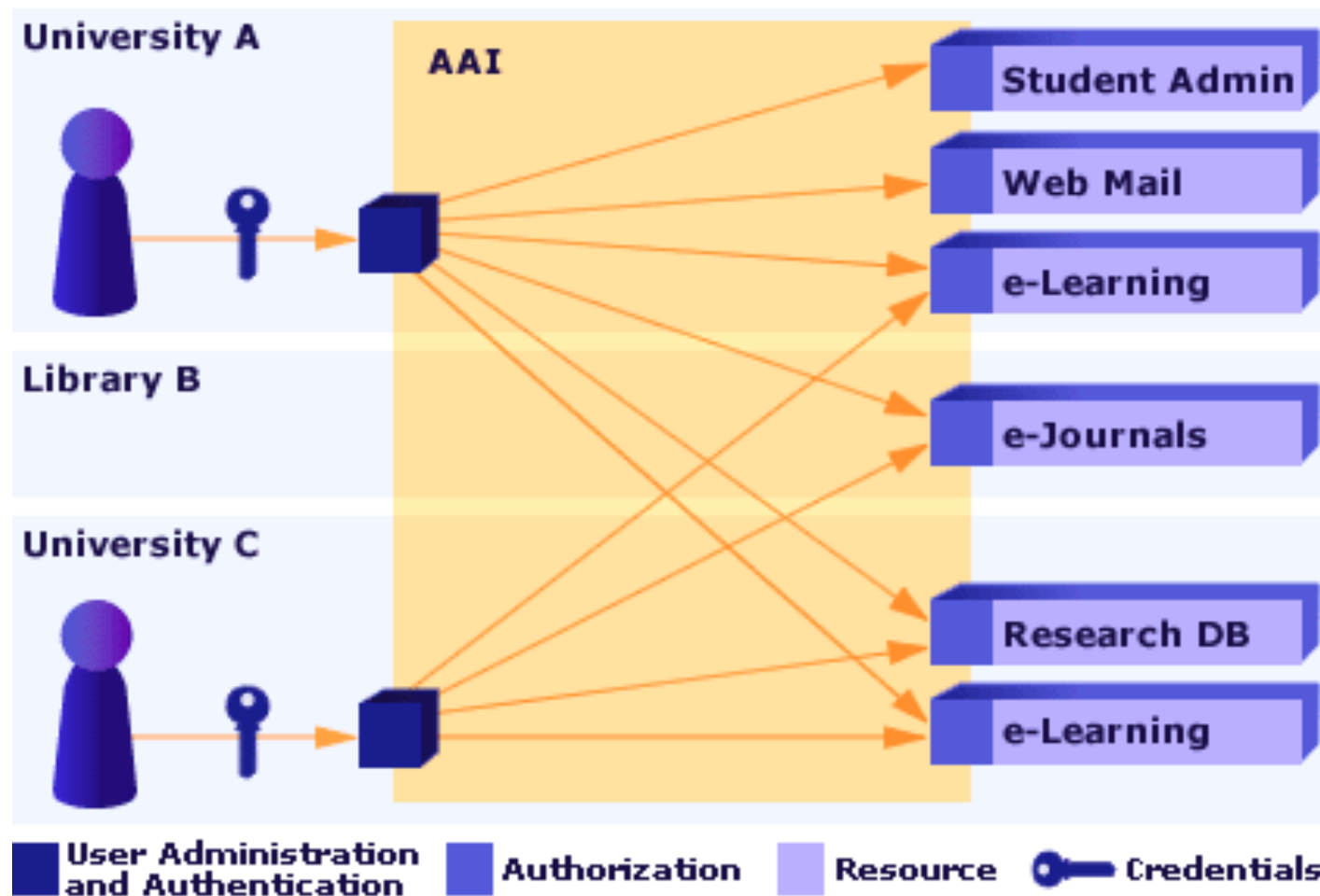


Federované přihlášení

- Rozšíření Single Sign-On konceptu přes více poskytovatelů identit
- Federované přihlášení službě umožní delegovat autentizaci na externí poskytovatele identit
- Oddělení autentizačního mechanismu od transportního
- Podpora přenosu autorizačních informací
- První viditelný zástupce: OpenID



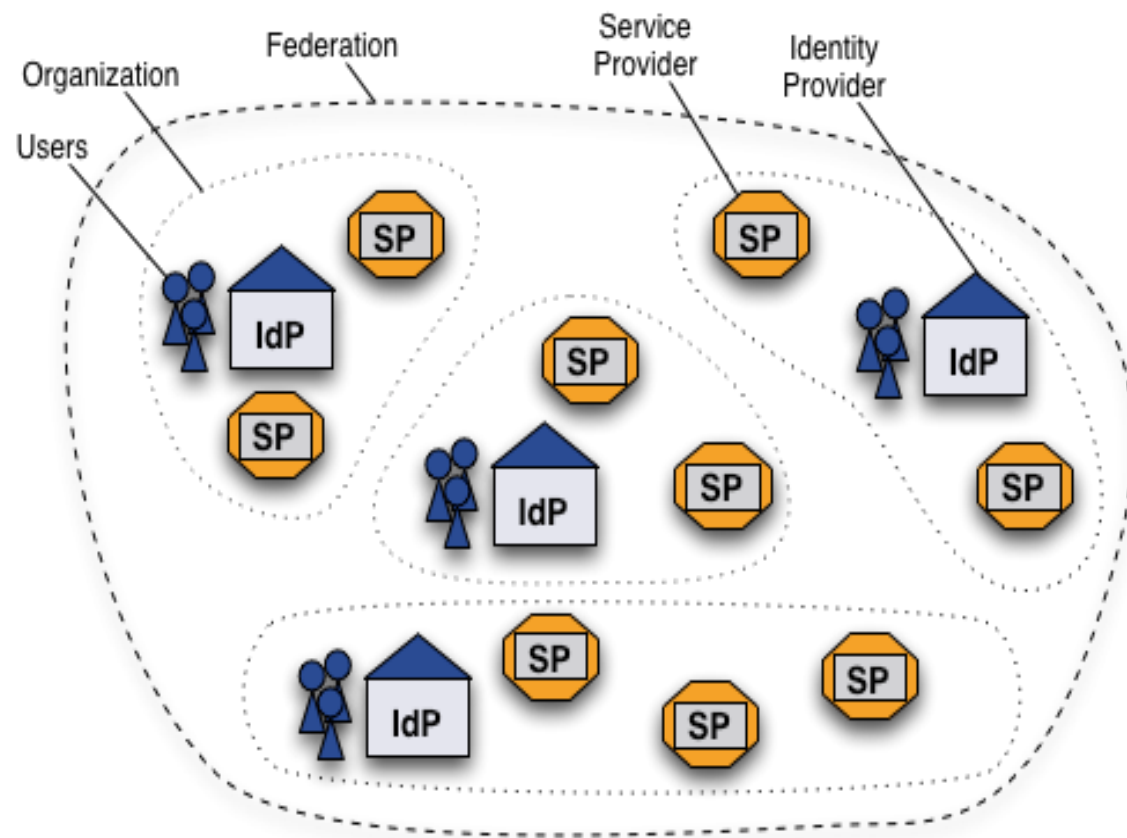
Federované přihlášení



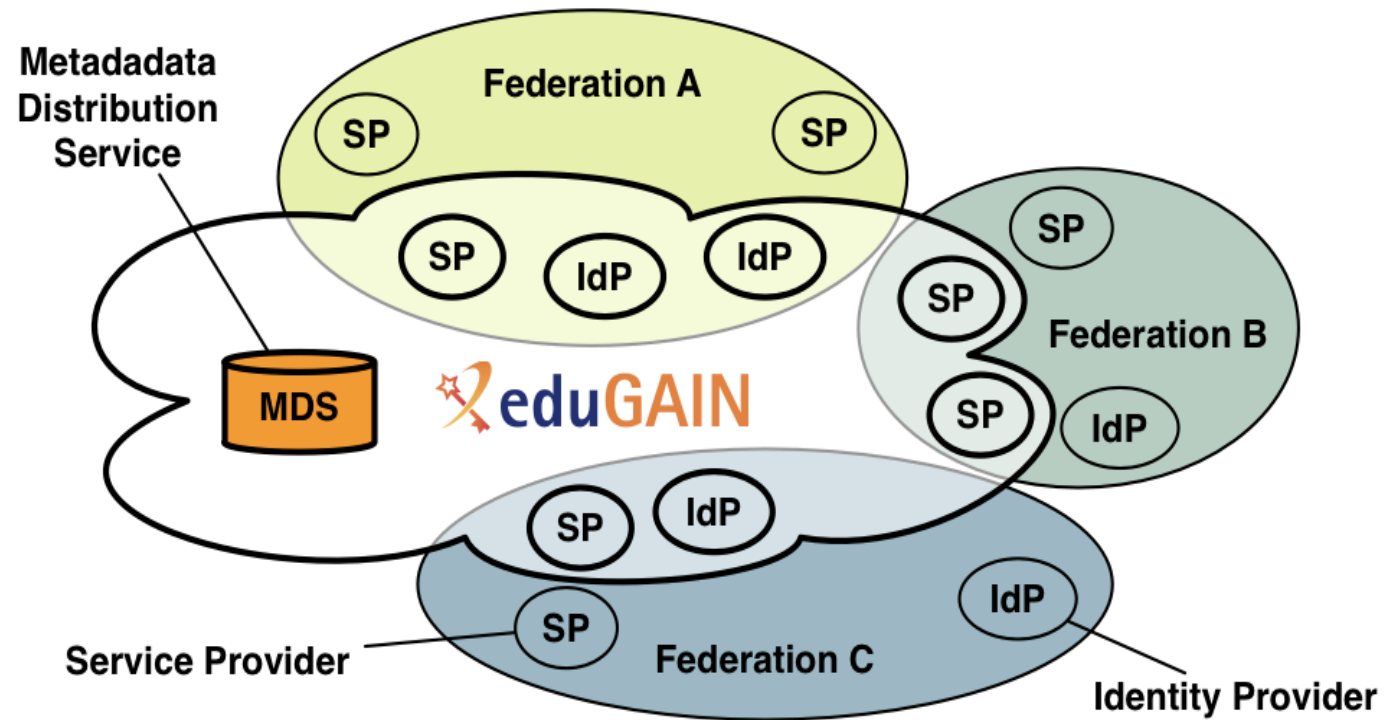
Federace identit

- Budování důvěry mezi entitami (SP, IdP)
 - Centrálně spravovaná
- Společná politika
- Harmonizace autorizačních dat
- V akademické sféře většinou jedna federace per stát

Schéma federace identit



eduGAIN – federace akademických federací



STORK



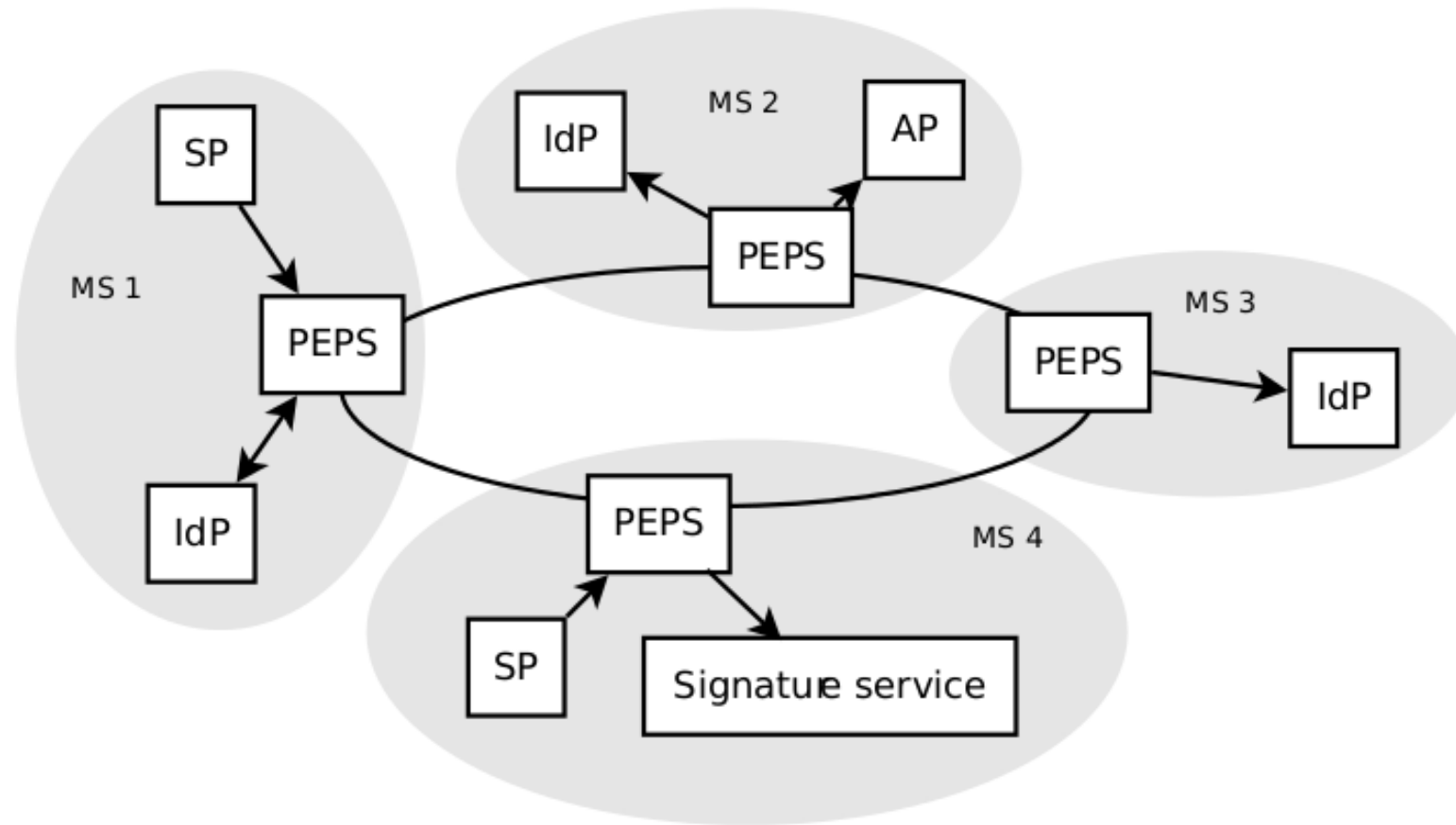
eIDAS

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (mj. ruší směrnici 1999/93/ES)
- Evropská legislativa upravující elektronickou identitu a služby vytvářející důvěru
 - Harmonizace přístupu
 - Standardizace komunikačních protokolů
 - Definice důvěry
- Cílem je umožnit obyvatelům EU využívat přeshraniční služby s vysokou mírou důvěry
 - Minimální zásah do realizace ve členském státě, nařízení specifikuje "rozhraní"

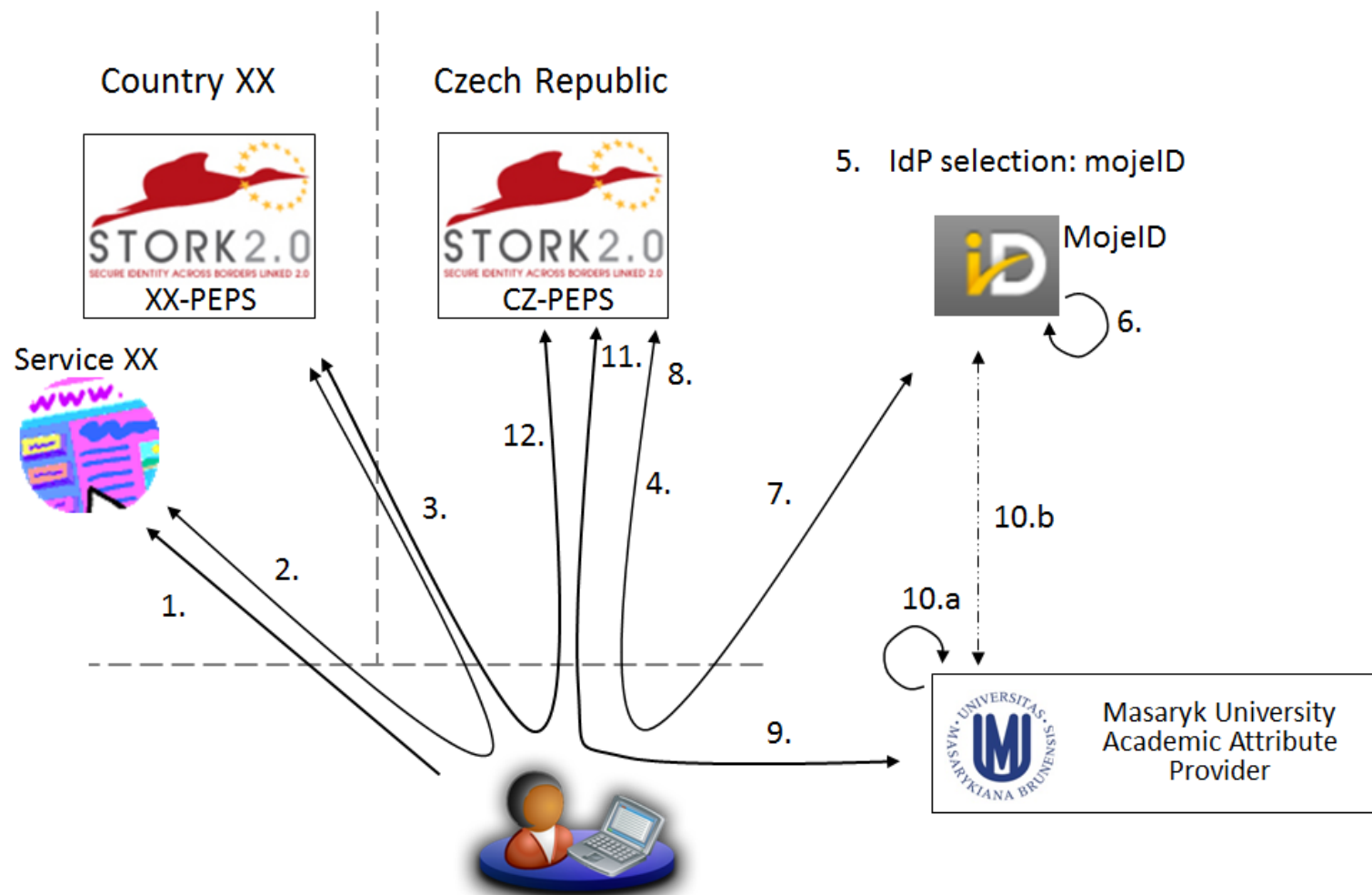
STORK pojmy

- PEPS - Pan European Proxy Services
- AP – Attribute Provider
- IdP – Identity Provider
- SP – Service Provider

STORK infrastruktura



STORK proces přihlášení



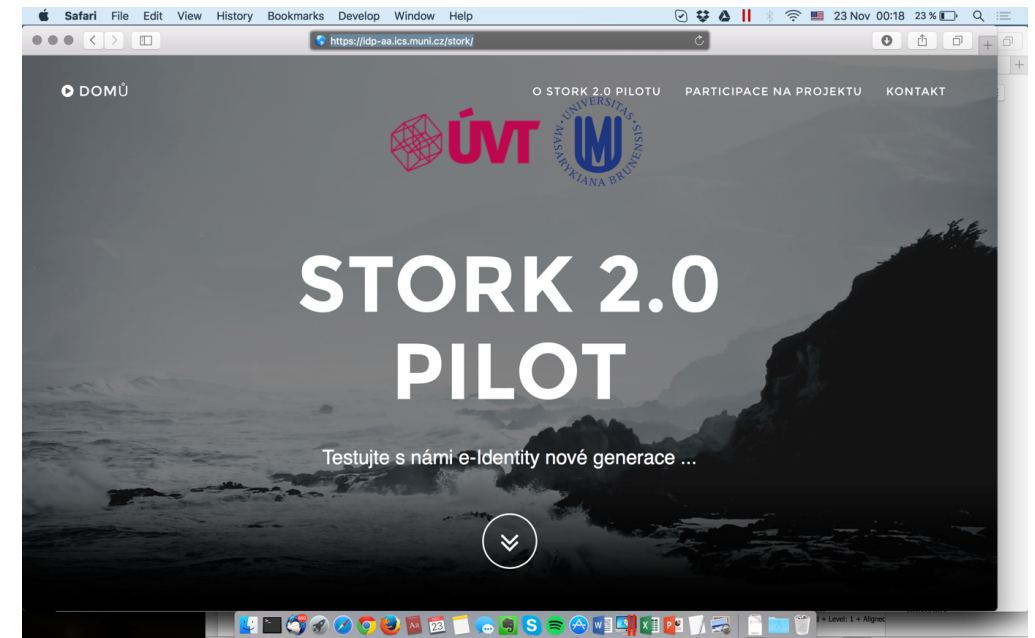
STORK technologie

- STORK využívá protokol SAML2 s vlastními úpravami
- Z možného výčtu flow využívá pouze frontendové
- Nepodporuje Single Sign-On
 - Single Sign-On je ponecháno na IdP

STORK - Důvěra

- Implicitní důvěra v PEPS
- Podpora úrovně důvěry v jednotlivé atributy

Projekt STORK2



Piloty

- eLearning and Academic Qualifications Pilot
- eBanking Pilot
- Public Services for Business Pilot
- eHealth Pilot

eLearning and Academic Qualifications Pilot

- Cílem bylo ověřit, zda se student dostane ke službám poskytovaným pouze studentům
- Virtuální předmět STORK101, který měl vyučující a studenty z různých zemí
- Integrace vysokých škol jako attribute provider
- Testování celého workflow
- Zpětná vazba od koncových účastníků
 - V případě MU, testováno na studentech

Identifikované problémy

STORK2.0
SECURE IDENTITY ACROSS BORDERS LINKED 2.0

STORK:: (Secure Identity Across Borders Linked)

Consent to request attributes

Service Provider DEMO-SP-CZ with QAA Level 3 is requesting the following attributes:

Attributes

Mandatory attribute(s)

- ☒ IsStudent
- ☒ Degree
- ☒ IsTeacherOf

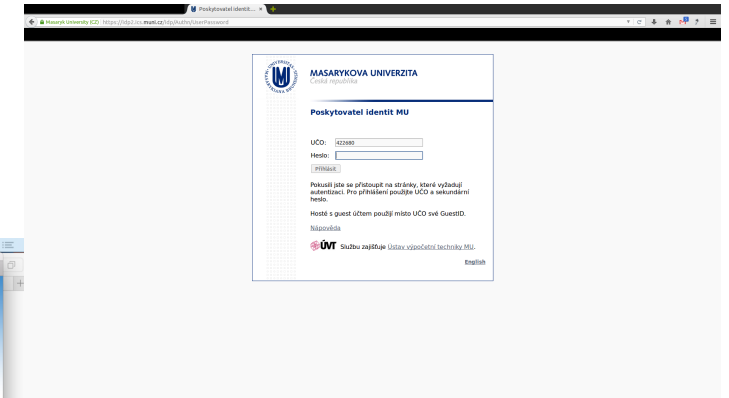
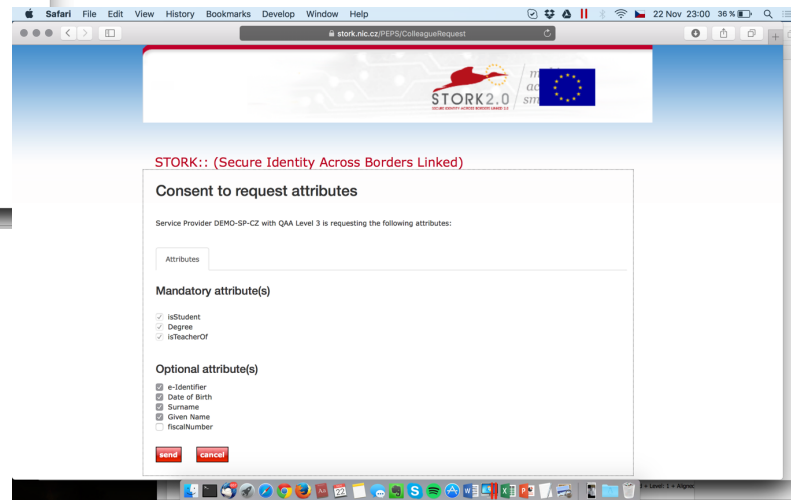
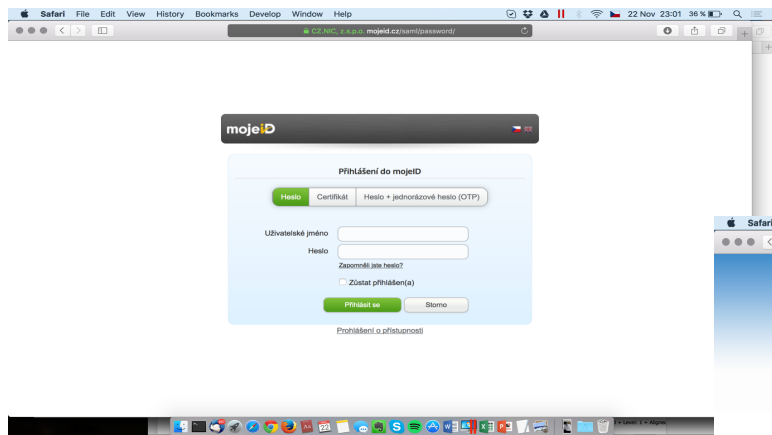
Optional attribute(s)

- ☒ e-Identifier
- ☒ Date of Birth
- ☒ Surname
- ☒ Given Name
- ☐ fiscalNumber

send **cancel**

Identifikované problémy

- Různé webové stránky z různým designem



Identifikované problémy

- Nejednoznačná sémantika atributů
 - Problém při mapování informací od AP
- Verze SAML2, která je specifická pro STORK
- Poskytovatelé atributů musejí ztotožnit uživatele
 - Pouze na základě jména a data narození, ostatní údaje musí dodat uživatel sám
- PEPS vidí vše a je single point of failure
- Dodané implementace jsou tristní

Přínosy

- Důvěryhodná identita osoby
 - Akademické instituce budou "jen" poskytovatelé atributů
- Dodatečné informace o osobě z autoritativních zdrojů
- Sjednocení technologií pro přenos autentizačních a autorizačních informací
- Legislativně podpořená aktivita

eID v ČR

- Zavádí elektronickou identifikaci občana
- Pro vybrané agendy nahradí datové schránky
- Poskytnout občanům elektronický přístup ke státním agendám
- Umožnit občanům využívat služby z jiných států EU



Stav eID v ČR

- Do nového občanského průkazu půjde nahrát digitální certifikát určený pro šifrování (podpora autentizace)
 - Kvalifikovaný digitální certifikát podporuje pouze digitální podpis
- Problém s výměnou stávajících OP
- Legislativa musí předcházet nasazení

Stav legislativy k eID v ČR

- Návrh adaptačního zákona k nařízení eIDAS pro oblast služeb vytvářejících důvěru
- Zavádí pojem **Národní certifikační autorita**
 - Identifikační certifikát
 - Provozovaná správou základních registrů

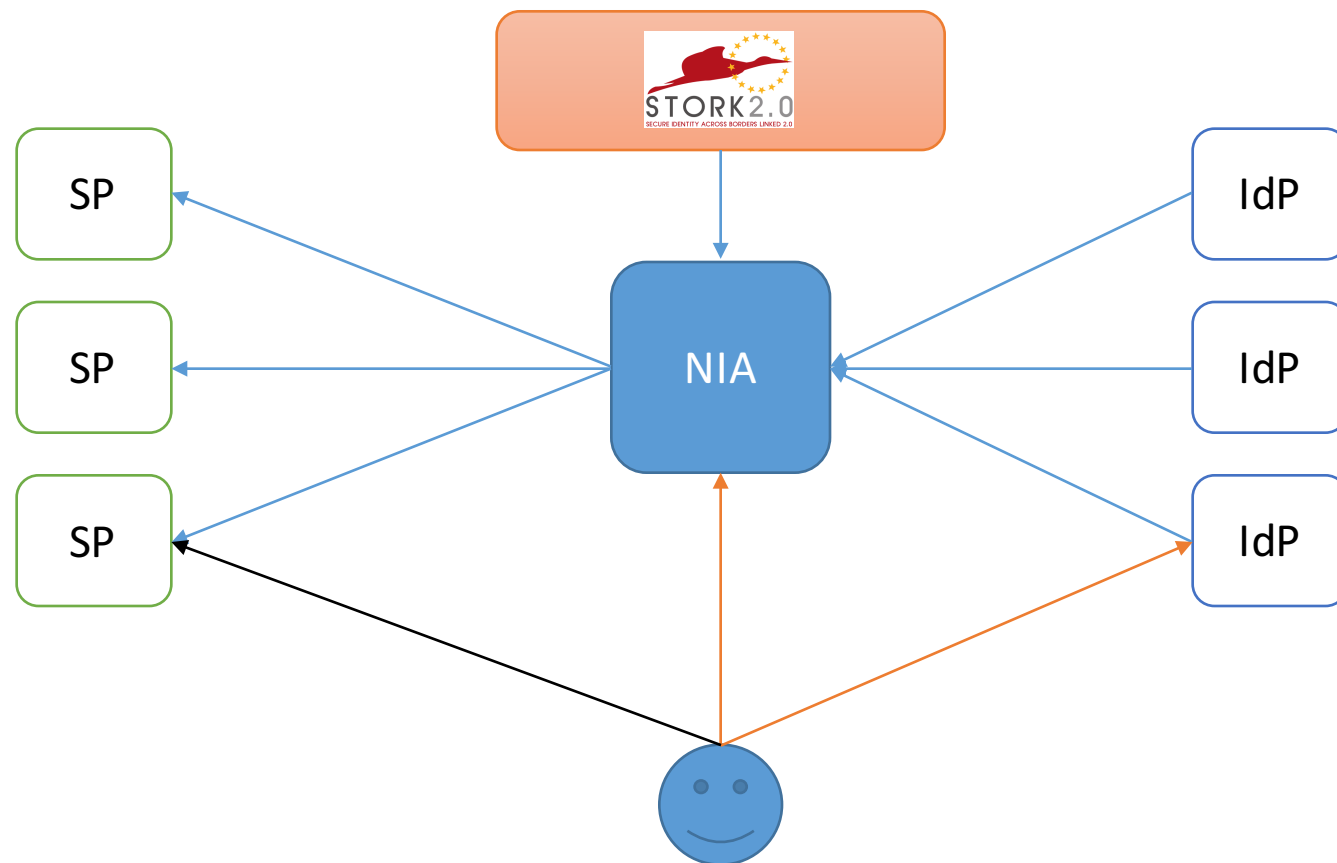
Stav legislativy k eID v ČR (2)

- Vládní návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů

Informační systém pro autentizaci

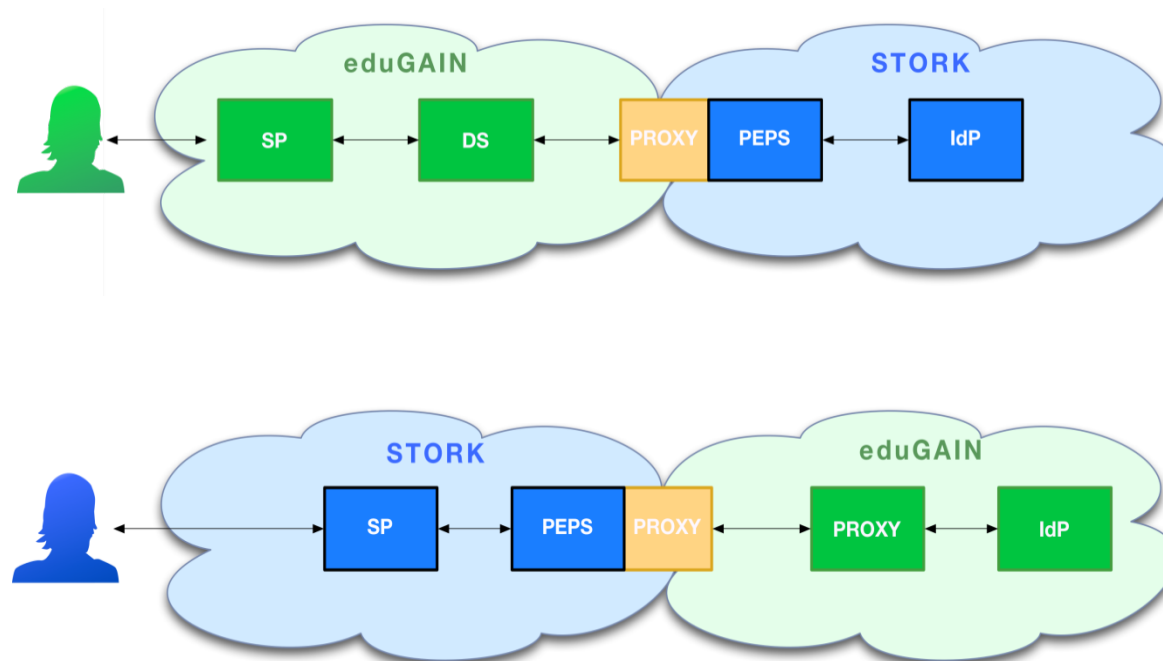
- **Narodní identitní autorita (NIA)**
- Autentizace držitele občanského průkazu (eOP)
 - Použití identifikačního certifikátu
- Uchovává pouze číslo OP a AIFO po dobu platnosti OP a 15 let po
 - Ostatní údaje čerpá ze základních registrů
- Provozována správou základních registrů

eIDAS (eID) v ČR



STORK a eduGAIN

- Snahy spojit existující akademické federace identit se STORK



Děkuji za pozornost

Michal Procházka

michalp@ics.muni.cz