

Novinky v autentizaci a autorizaci

Martin Kuba <makub@cesnet.cz>

Oddělení autentizační a autorizační infrastruktury

konference e-infrastruktury CESNET, 30.9.2026

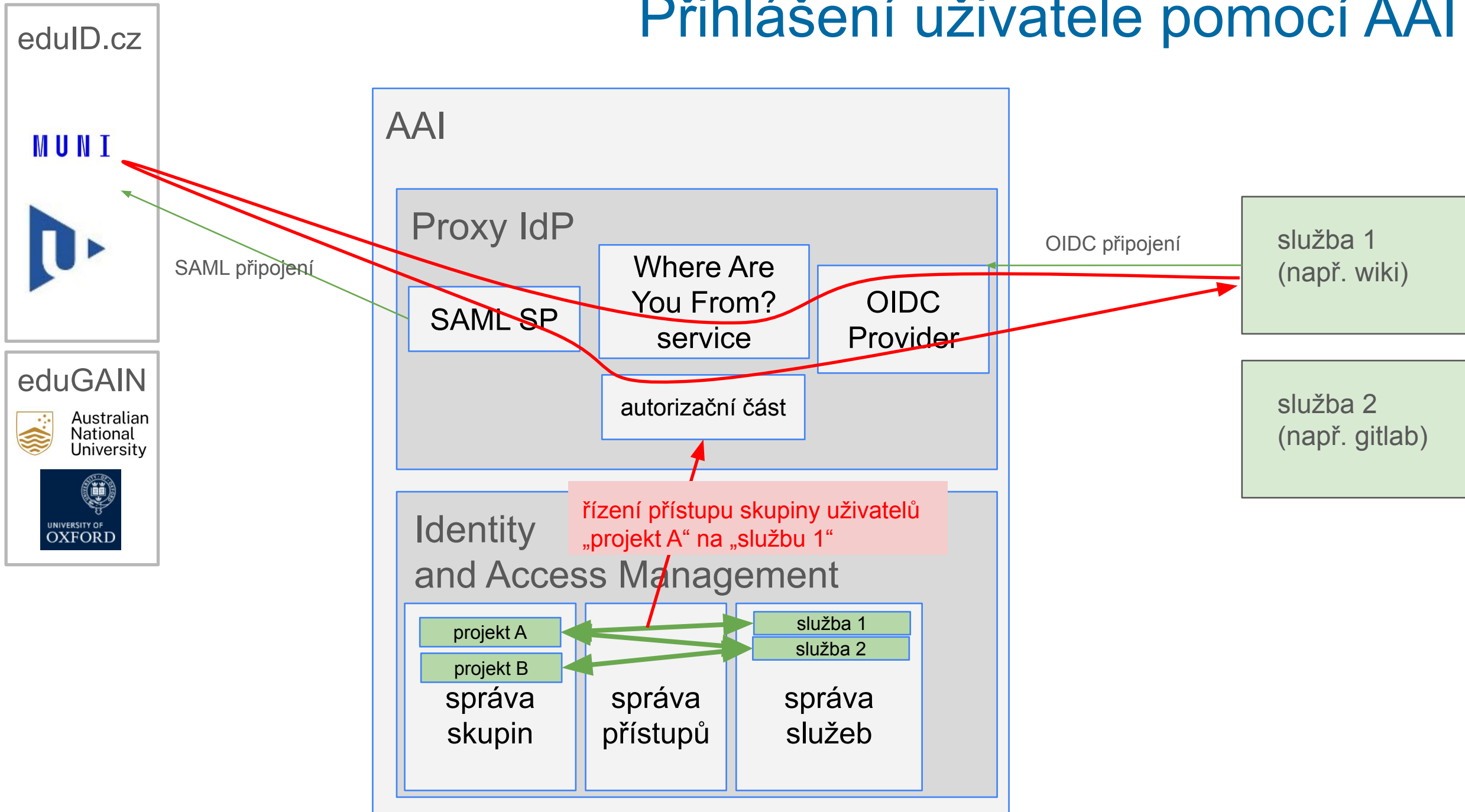
- **autentizace** - ověření proklamované identity subjektu
 - osoby uživatele, web serveru, softwarového agenta, ...
- **autorizace** - umožnění přístupu subjektu k něčemu
 - datům, počítačům, software, přístrojům, ...
- **AAI** - autentizační a autorizační infrastruktura
 - softwarový systém poskytující A+A v prostředí, kde uživatelé a využívané prostředky jsou z více různých organizací
 - typicky společné projekty a konsorcia více univerzit, výzkumných ústavů, případně komerčních firem



- Identity and Access Management (IAM)
 - systém pro správu a distribuci dat potřebných pro provádění autorizací na spravovaných výpočetních prostředcích
- Proxy Identity Provider (Proxy IdP)
 - Where Are You From Service (WAYF) - služba pro výběr domovské organizace / IdP uživatele
 - proxy přenáší autentizaci mezi původním IdP a on-line službou
 - doplňuje údaje potřebné pro autorizaci na on-line službě, nebo provádí autorizaci sama
 - překlad mezi protokoly (SAML, OAuth 2, OIDC)



Přihlášení uživatele pomocí AAI



- e-infrastruktura CESNET
 - Datová úložiště
 - videokonference Zoom
- e-INFRA CZ
 - služby e-INFRA CZ - MetaCentrum, AI, OpenStack, Kubernetes
 - externí služby core facilities - CEITEC, VMCF Viničná
- Národní Repozitářová Platforma NRP
 - repozitáře (Herbarium, Archeo Vault, ...)
 - podpůrné služby
- EOSC CZ Node
 - český národní uzel European Open Science Cloud
 - propojení s dalšími uzly - tématickými (LifeScience, BBMRI), národními (Itálie, Německo, Finsko, ...) a infrastrukturními (EGI, GÉANT)



spojení výše uvedených AAI do jednotné nové značky CESiD -
Czech Educational and Scientific iDentification



CESiD

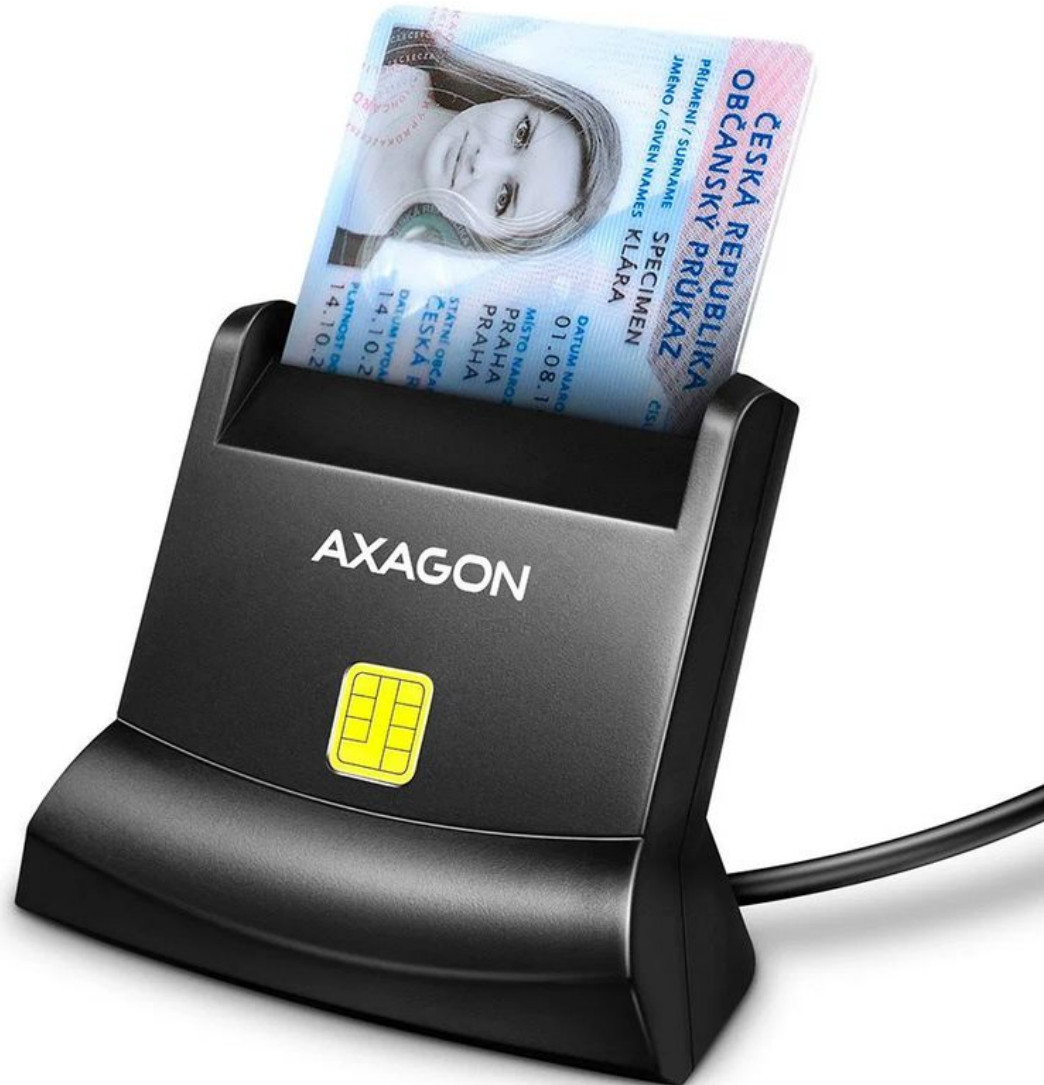


- stabilní, na projektech nezávislé řešení, které národním uživatelům a službám poskytuje sjednocující platformu pro různé projekty a infrastruktury
- integrace na evropské a mezinárodní úrovni
- nová technologie pro Proxy IdP - Apereo CAS
- věčná DNS doména cesid.cesnet.cz kvůli Passkeys
- připojení na nové IdP s vyššími LoA
 -  **Bank iD** - úroveň ověření eIDAS substantial (značná)
 -  **mojeiD** - úrovně ověření eIDAS substantial (značná) a high (vysoká)



- míra ověření skutečné totožnosti uživatele (identity proofing)
 - nízká - sám prohlásil kdo je
 - značná - byl ověřen (např. ukázal občanský průkaz přes video)
 - vysoká - byl fyzicky přítomen při ověření
- síla vazby mezi osobou uživatele a technickým způsobem autentizace
 - nízká - jedním faktorem (např. heslo)
 - značná - dvěma faktory (např. aplikace v mobilu a otisk prstu)
 - vysoká - dvěma faktory s čipem certifikovaným pro odolnost vůči fyzickému útoku (např. eObčanka + kód IOK)





Levels of Assurance - eIDAS / ISO 29115

	LOW	SUBSTANTIAL		HIGH	eIDAS Definition	
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 3	LEVEL 4	ISO 29115
	Weak Authentication <i>Legacy Password</i>	Secure Authentication - Seamless - SMS+URL - USSD - SIM Applet - Smartphone App - Token or OTP	Strong Authentication - USSD - SIM Applet - Smartphone App - Token OTP + pw - Biometrics	Strong Authentication - SIM Applet - Smartphone App in TEE - Token OTP (PIN + certified TEE or SE) - Biometrics	Very Strong Authentication - SIM Applet with PKI - Smartphone App in TEE with PKI - PKI eID (PIN) - PKI ID (PIN + SE (SIM /eSE) - Biometrics	Authentication / electronic ID
	No Identity Proofing	Presentation of identity information	Verification of Identity information		In-person registration with verification	Identity Proofing During Registration
	EXTREMELY HIGH MITIGATED LOW MINIMAL MINIMAL					Risk Level

- poskytuje LoA 3 podle standardu ISO/IEC 29115:2013
- odpovídá LoA eIDAS „substantial“ (značná)
- úrovně služby
 - BankID Connect - jméno, telefon, email
 - BankID Identify - navíc adresu, tituly, pohlaví, rodné číslo, bankovní účet
 - BankID Identify Plus - místo narození, stav, doklad totožnosti, právní status
 - BankID AML - Anti-Money-Laundering zákon č. 253/2008 Sb.
- pro uživatele s účtem v jedné ze zapojených bank
 - Česká spořitelna vydává dětem od 7 let
 - ostatní banky od 15 let
 - čeští občané a cizinci, kteří mají osobní doklad vydaný českým státem
- potenciálně miliony uživatelů



- poskytovatel totožnosti pro eIDAS eID („identita občana“)
- úrovně ověření:
 - značná - je potřeba:
 - mobilní aplikace MojelD
 - ověření totožnosti mobilní aplikací Mobilní klíč eGovernmentu, datovou schránkou, NIA ID, nebo návštěvou pobočky CzechPoint na poště
 - vysoká - je potřeba:
 - USB token s certifikacemi FIDO Level 2 a FIPS nebo CC EAL6+ schválený DIA
 - ověření totožnosti eObčankou, čipovou kartou Starcos od I.CA, nebo návštěvou pobočky CzechPoint na poště
- pro uživatele s účtem v MojelD
 - čeští občané
 - pro občany Slovenska funguje fyzické ověření na CzechPointu, nefunguje on-line ověření slovenským eID





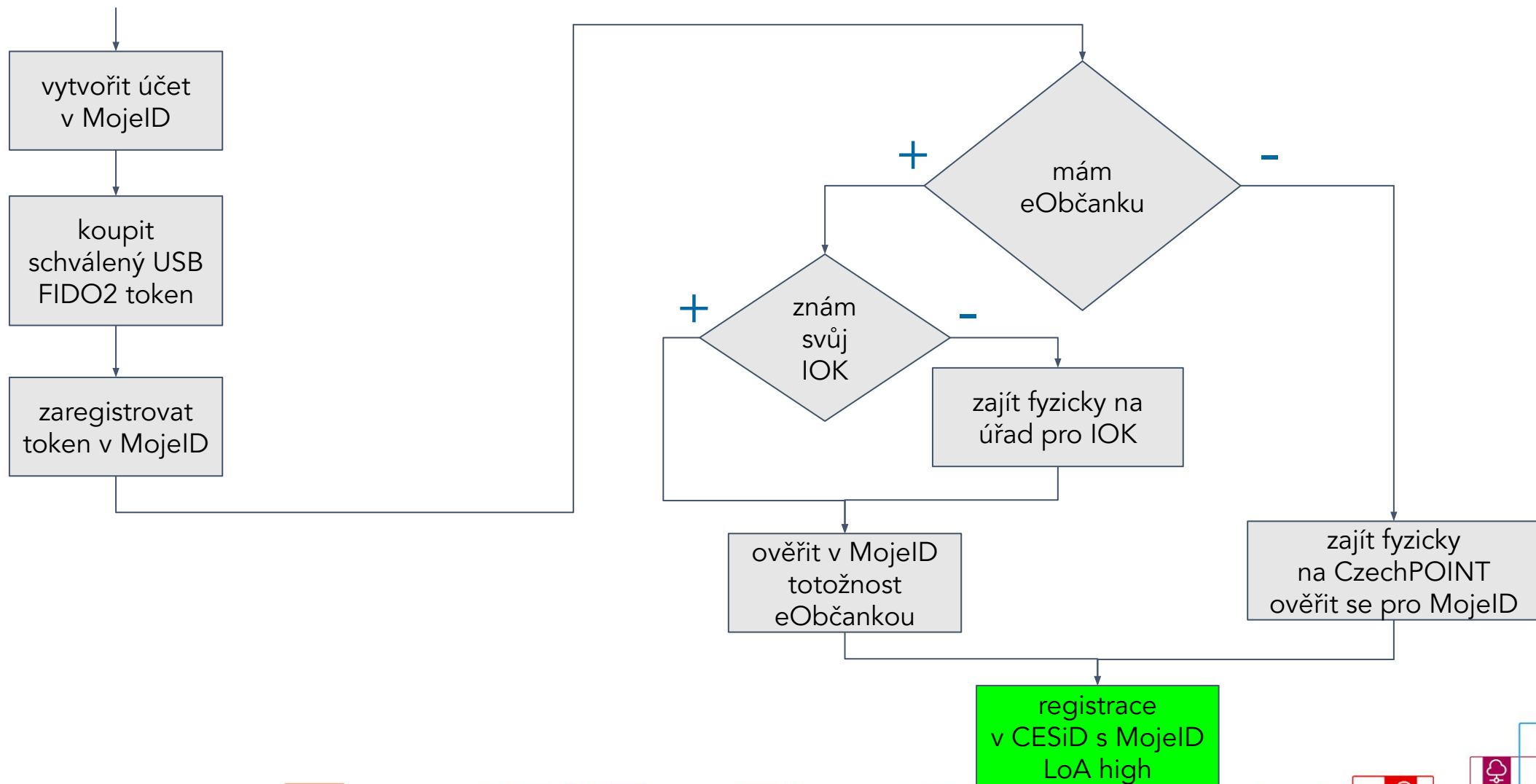
Předání údajů z MojeID

CESiDPřihlásit
se k:Czech Educational and
Scientific
iDentification[Zásady ochrany
soukromí](#)[Podmínky
služby](#)Přihlásit se jako: **makub**

Další předávané údaje

- ☐ Jméno: Martin
- ☐ Příjmení: Kuba
- ☐ Přezdívka: Makub
- ☐ Pohlaví: M
- ☐ Celé jméno: Martin Kuba

Jak v CESiD získat LoA eIDAS high



Token2 PIN+ Release3.3



GoTrust Idem Key



Yubikey 5.7 a FIPS 5.4



- podrobnosti zítra v sekci Bezpečnost
- podle nařízení EU má každý členský stát na konci roku 2026 poskytovat občanům EUDIW
- není to peněženka, je to dokladovka, bude obsahovat doklady
 - kvalifikované
 - občanský průkaz
 - řidičský průkaz, technický průkaz auta
 - ISIC, univerzitní diplom
 - průkaz zdravotního pojištění
 - nekvalifikované
 - členská karta do fitness klubu
 - karta zaměstnance
 - vlaková jízdenka, letenka



- wallet je aplikace (mobilní nebo webová)
 - sbírá doklady od vydavatelů (Issuer)
 - vydává doklady příjemcům (Verifier)
- vydavatel nemůže sledovat, kde byl doklad použitý
- protokoly OID4VC (OpenID for Verifiable Credentials)
- doklady obsahují veřejný klíč peněženky
 - nemůže je předložit jiná peněženka (nedají se ukrást)



- autorizační model ABAC (Attribute Based Access Control)
- silnější než RBAC (Role Based Access Control)
- pravidla na základě atributů subjektu, objektu, operace a prostředí
- např. „přístup k záznamům pacienta může mít lékař jedoucí s ním v sanitním voze“
- „být zároveň v sanitním voze“ je atribut prostředí
- OPA je open-source cloud-native první použitelná implementace ABAC
- hledáme reálné případy využití, na které nestačí RBAC



- CESiD je na projektech nezávislé AAI
- vyšší LoA připojením CESiD na BankID a MojeID
- peněženka EUDIW má být na konci roku funkční
- OPA implementace ABAC je připravena k použití

