National Czech Programme | eosc

Iniciální architektura AAI pro NRP

Základní informace

Název dokumentu	Iniciální architektura AAI pro NRP
Registrační číslo projektu	CZ.02.01.01/00/23_014/0008787
Název KA	4.3 – Řízení přístupu k datům
Číslo a název výstupu	14 – Iniciální architektura AAI pro NRP
Zodpovědná osoba	Mgr. Peter Lényi
Licence dokumentu	

Spolufinancováno Evropskou unií

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Národní repozitářová platforma pro výzkumná data (NRP)
CESNET, zájmové sdružení právnických osob
Korespondenční adresa: Generála Píky 430/26, 160 00 Praha
info@eosc.cz; www.eosc.cz

Autoři

Instituce	Jméno a příjmení	ORCID	Email
MU	Peter Lényi	https://orcid.org/0009-0009-7840-5458	lenyi@ics.muni.cz
CESNET	Pavel Vyskočil	https://orcid.org/0000-0001-8376-2761	pavel.vyskocil@cesnet.cz
VŠB	Lukáš Vojáček	https://orcid.org/0000-0002-7448-3477	lukas.vojacek@vsb.cz

Seznam použitých zkratek

AAI	Autentizační a autorizační infrastruktura
AAL	Důvěra v sílu autentizace
ABAC	Řízení přístupu na základě atributů
EOSC	angl. *European Open Science Cloud*
FAIR	angl. *Findable*, *Accessible*, *Interoperable*, *Reusable*
FAL	Důvěra v zabezpečení federace
IAL	Důvěra v proces ověření totožnosti
IdM	Správa identit
IdP	Poskytovatel identit
MFA	Vícefázové ověření
NDI	Národní datová infrastruktura
NRP	Národní repozitářová platforma
PAP	angl. *policy administration point*
PDP	angl. *policy decision point*
PEP	angl. *policy enforcement point*
PII	Osobní údaje
PIP	angl. *policy information point*
R/S NRP	Repozitáře a/nebo služby NRP
RBAC	Řízení přístupu na základě rolí
SD	Citlivá data
SLO	Jednotné odhlášení
SP	Poskytovatel služby
SSO	Jednotné přihlášení
VO	Virtuální organizace

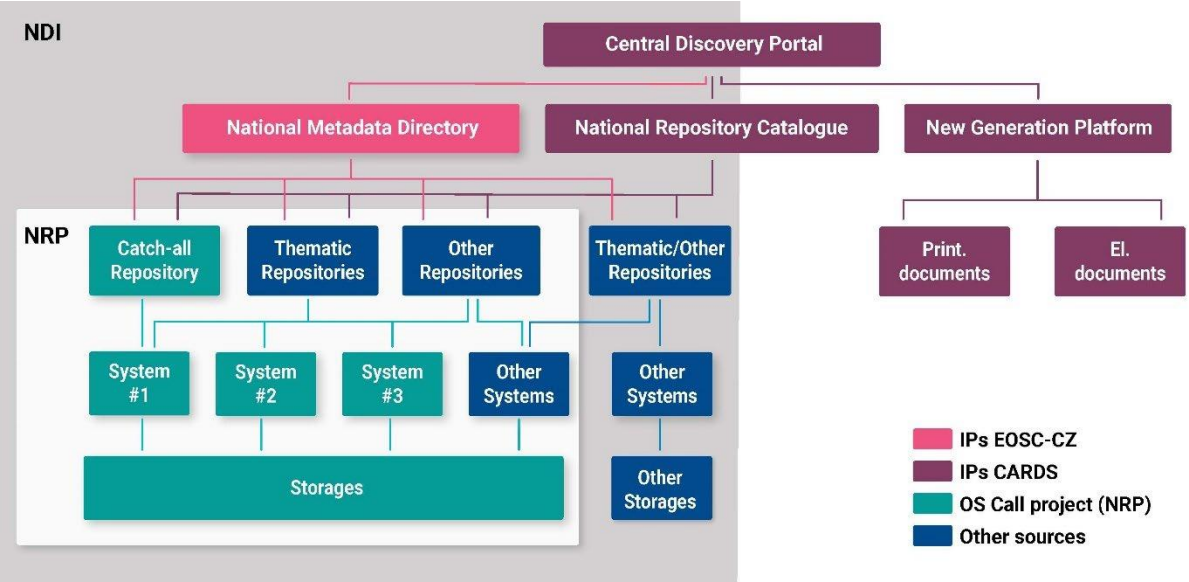
Obsah

Shrnutí

Tato technická zpráva je plánovaným výstupem č. 14 projektu NRP. Popisuje iniciální architekturu autentizační a autorizační infrastruktury (dále jen AAI) v kontextu NRP. Hlavní cílovou skupinou této zprávy jsou vývojáři a správci pilotních repozitářů a služeb NRP, kteří se s ní musí obeznámit před připojením svých systémů k AAI řešení.

Úvod

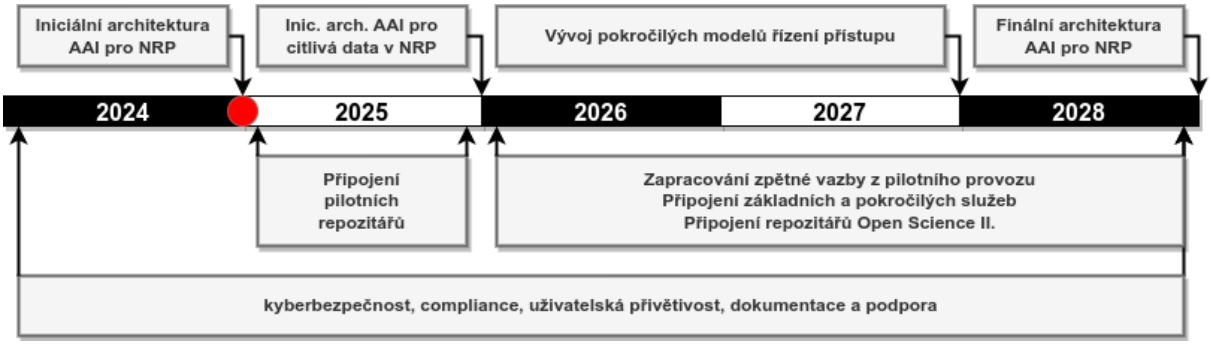
Národní repozitářová platforma pro výzkumná data (dále jen NRP) nabídne českým vědcům moderní prostředí pro ukládání a správu vědeckých dat prostřednictvím specializovaných datových repozitářů a souvisejících služeb. Platforma podpoří vědeckou komunitu při uchovávání kvalitně anotovaných dat opatřených metadaty, která budou snadno vyhledatelná, přístupná, interoperabilní a opakovaně použitelná v souladu s principy FAIR. NRP je součástí komplexního prostředí NDI, které bude v rámci implementace EOSC v ČR realizováno.[1]



Obrázek 1: Ekosystém služeb e-infrastruktury [2]

Tato technická zpráva je plánovaným výstupem č. 14 projektu NRP. Popisuje iniciální architekturu autentizační a autorizační infrastruktury (dále jen AAI) pro NRP – a v širším kontextu pro EOSC CZ. Publikuje se po prvním roce pětiletého projektu. Ve druhém roce na ni navazuje připojení pilotních repozitářů NRP k AAI řešení a technická zpráva Iniciální architektura AAI pro citlivá data v NRP. Cílem zbylých tří let projektu je návrh pokročilých modelů řízení přístupu, zapracování zpětné vazby z pilotního provozu NRP, připojení základních a pokročilých služeb NRP a nových repozitářů z projektu Open Science II[3].

[1] https://www.eosc.cz/o-nas/faq#NDI
[2] Zdroj: Základní obsah projektu NRP, str. 7
(odkaz na stažení) https://www.eosc.cz/media/3713976/nrp_zakladni_obsah_projektu_2024.pdf
[3] https://opjak.cz/vyzvy/vyzva-c-02_24_030-open-science-ii/



Obrázek 2: Harmonogram AAI pro NRP [4]

Zpráva začíná tímto úvodem a definicemi odborných termínů a příslušných zkratek v první kapitole. Druhá kapitola se věnuje struktuře řešení AAI pro NRP a integracím. Ve třetí kapitole jsou popsané povinné autentizační funkce AAI a ve čtvrté iniciální model řízení přístupu pro repozitáře a služby NRP. Poslední, pátá kapitola obsahuje výčet podpůrných funkcí AAI.

Hlavní cílovou skupinou této zprávy jsou vývojáři a správci pilotních repozitářů a služeb NRP, kteří se s ní musí obeznámit před připojením svých systémů k AAI řešení. Autorem zprávy je skupina řešitelů **NRP KA 4.3** [5].

[4] Zdroj: Studie proveditelnosti NRP, str. 64-65, 91
(odkaz přístupný pouze registrovaným řešitelům projektu NRP)
https://researchinfracz.sharepoint.com/:b:/r/sites/NRP/Sdilene%20dokumenty/General/Studie%20proveditelnosti/NRP_Studie_proveditelnosti.pdf
[5] nrp-ka4-3-data-access@eosc.cz

1 Terminologie

1.1 AAI

Autentizační a autorizační infrastruktura (AAI) je sada technických komponent a souvisejících procesů, který slouží k ověření digitální identity uživatele (autentizaci), aby bylo možné tomuto uživateli přidělit oprávnění (autorizace), což umožňuje na jednu stranu chránit a na druhou stranu sdílet data, služby, přístroje atp.

Perun AAI [6] je komplexní open-source softwarové řešení, kombinace existujících open-source komponent a vlastního vývoje, které představuje technický základ postavený na mezinárodních standardech potřebný pro provoz AAI, primárně ve federovaném prostředí akademických institucí a výzkumných infrastruktur.

Perun IdM je jedna ze dvou hlavních komponent Perun AAI. Zajišťuje zejména správu identit a přístupů uživatelů: udržuje databázi digitálních identit uživatelů, umožňuje je zařazovat do virtuálních organizací a skupin, umožňuje skupiny přiřazovat ke zdrojům a propagovat data z těchto objektů poskytovatelům služeb, kteří je můžou využít pro lokální autentizaci či řízení přístupu.

Perun ProxyIdP je jedna ze dvou hlavních komponent Perun AAI. Zajišťuje zejména autentizaci uživatele a částečné řízení přístupu: slouží jako centrální uzel, přes který si poskytovatelé služeb a identit vyměňují autentizační požadavky a odpovědi, které umí obohatit o uživatelská data z Perun IdM, a drží relace pro zabezpečení funkcí jednotného přihlášení a odhlášení.

EOSC CZ AAI je instance AAI, postavená na technickém řešení Perun AAI, provozovaná sdružením CESNET[7] pro potřeby implementace EOSC v ČR, např. NRP.

[6] https://perun-aai.org/
[7] https://www.cesnet.cz/

Poskytovatel identit (angl. *identity provider*, **IdP**) je softwarová aplikace nebo služba, která autentizuje uživatele a vydává informace o jejich identitě poskytovatelům služeb. Poskytovatel identit je odpovědný za ověření uživatelovy digitální identity jedním nebo více faktory (např. jméno/heslo, biometrie) a zabezpečuje mechanismus jednotného přihlášení a odhlášení. [8]

Poskytovatel služby (angl. *service provider*, **SP**) je softwarová aplikace nebo služba, která poskytuje přístup ke zdrojům nebo službám uživatelům, kteří byli autentizováni poskytovateli identit. Poskytovatel služby je (obvykle) odpovědný za rozhodování, ke kterým zdrojům nebo službám mají uživatelé přístup, a pak vyhodnocování autorizačních pravidel (nebo může řízení přístupu delegovat na AAI). V kontextu NRP jsou poskytovateli služeb repozitáře a služby NRP. [9]

Provisioning uživatele (angl. *user provisioning*) je proces zpřístupnění IT zdrojů anebo digitálních objektů uživateli na základě jeho digitální identity (či účtu) a autorizačních pravidel. Provisioning v širším významu zahrnuje i proces aktualizace při změně. Analogicky existuje i **deprovisioning uživatele** (angl. *user deprovisioning*), proces odebrání všech oprávnění. [10]

Provisioning a deprovisioning může probíhat ve dvou variantách. Ve variantě *just-in-time,* to je interaktivně během přihlášení uživatele, nebo ve variantě *just-in-case,* to je automaticky a dle potřeby (při každé změně, denně o půlnoci atp.).

Virtuální organizace (angl. *virtual organization*, **VO**) je soubor osob nebo institucí, které sdílejí zdroje (hardware, služby, data aj.) za účelem spolupráce. Majitelé, poskytovatelé a spotřebitelé zdrojů ve VO společně definují, kdo, co a jak může sdílet. [11]

V kontextu Perun AAI je VO množinou uživatelů, kteří společně jednají s poskytovateli služeb, dostávají do užívání zdroje a sami si řídí, kdo jsou členové VO a mají k nim přístup.

[8] (anglicky) https://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf (ř. 201)
[9] (anglicky) https://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf (ř. 361)
[10] (anglicky) https://en.wikipedia.org/wiki/Provisioning_(technology)#User_provisioning
[11] (anglicky) https://arxiv.org/abs/cs/0103025

1.2 NRP

Národní repozitářová platforma pro výzkumná data (**NRP**)[12] nabídne českým vědcům moderní prostředí pro ukládání a správu vědeckých dat prostřednictvím specializovaných datových repozitářů a souvisejících služeb. Platforma podpoří vědeckou komunitu při uchovávání kvalitně anotovaných dat opatřených metadaty, která budou snadno vyhledatelná, přístupná, interoperabilní a opakovaně použitelná v souladu s principy FAIR[13].

Repozitář je technické, personální a procesní zajištění dlouhodobého úložiště pro ukládání a publikaci citovatelných digitálních objektů, které patří vědecké skupině nebo instituci.

Repozitářový systém je softwarový balík, na kterém lze provozovat repozitáře. V rámci NRP jsou k dispozici tři základní repozitářové systémy s vyšší úrovní podpory: CESNET Invenio, CLARIN-DSpace a ASEP/ARL. Repozitáře ale mohou být v NRP provozovány i na jiných, alternativních systémech, např. Islandora.

Základní a pokročilé služby NRP jsou sadou nástrojů a služeb vyvíjených pro potřeby NRP, tj. pro správu metadatových profilů, podporu práce s licencemi, řízení přístupu k datům (mj. AAI), podporu strojového zpracování dat a metadat, plánování správy dat, automatizaci sběru dat a metadat, integraci výpočetních *workflows*.[14]

Repozitáře a služby NRP (**R/S NRP**) je souhrnné označení pro repozitáře NRP a základní a pokročilé služby NRP.

[12] https://www.eosc.cz/o-nas/narodni-podpora-pro-eosc/nrp
[13] (anglicky) doi.org/10.1038/sdata.2016.18
[14] Roadmapa služeb NRP (na stránce dole):
https://www.eosc.cz/projekty/narodni-repozitarova-platforma-pro-vyzkumna-data-os-i-nrp/nrp
(filtry: spravuji FAIR data, rozšířená časová osa, všechny projekty, nástroje a služby)

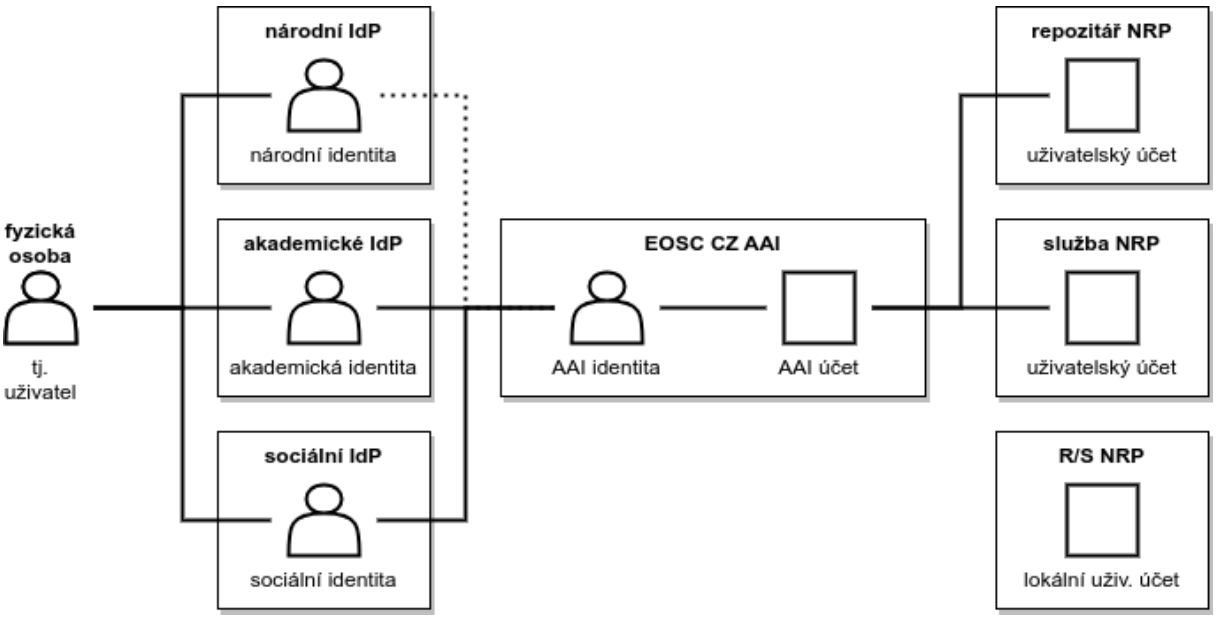
1.3 Identity

Uživatel (angl. *user*) je pro účely této technické zprávy definován jako fyzická osoba, která používá softwarový systém (R/S NRP, EOSC CZ AAI) a vystupuje přitom pod nějakou digitální identitou.

Digitální identita (angl. *digital identity*) je soubor dat v počítačovém systému, který v něm identifikuje uživatele. Obvykle, ale ne nutně, to jsou osobní údaje. Jeden uživatel má typicky několik různých digitálních identit. [15]

Uživatelský účet (angl. *user account*) je soubor dat v softwarovém systému s vazbou na digitální identitu. Obvykle to jsou osobní údaje, systémová nastavení a další informace, které se pak používají pro přístup k funkcím daného softwarového systému. Jeden uživatel má typicky mnoho různých uživatelských účtů v různých systémech.

Servisní účet (angl. *service account*) je reprezentace neosobního (obvykle strojového) přístupu v konkrétním softwarovém systému. Má svou vlastní digitální identitu nezávislou na digitálních identitách uživatelů, kteří jej spravují.



Obrázek 3: Ilustrace vztahu mezi uživatelem, digitální identitou a uživatelským účtem

[15] (anglicky) https://en.wikipedia.org/wiki/Digital_identity

Identity proofing (nepřekládáme) je proces ověření, že je uživatel konkrétní fyzickou osobou. Toto ověření lze provést různými způsoby, které pak vedou k různé *identity assurance*. [16]

Identity assurance (nepřekládáme) je míra důvěry v tvrzení, že je zkoumaná identita spojená s konkrétní fyzickou osobou, resp. míra důvěry ve způsob ověření totožnosti (**IAL**), sílu autentizace (**AAL**) a zabezpečení federace (**FAL**). [17]

Identity freshness (nepřekládáme) je míra, nakolik jsou digitální identita a přidružené atributy aktuální. Obvykle se vyjadřuje jako čas, který uplynul od posledního ověření totožnosti nebo získání atributů z autoritativního zdroje. [18]

Identity provenance (nepřekládáme) je dokumentace původu digitální identity. V širším významu to je celý řetězec důkazů od vzniku digitální identity po její aktuální použití. [19]

[16] Definice se různí, za autoritativní zdroj považujeme:
(anglicky) doi.org/10.6028/NIST.SP.800-63-3
[17] (ibid.)
[18] Zde nabízíme vlastní definici, protože termín *freshness*, resp. last refresh, se zmiňuje jen ve dvou publikacích (o nichž víme), a i to jen ve vztahu k atributům vydaným při autentizaci:
(anglicky) doi.org/10.6028/NIST.IR.8112
(anglicky) https://refeds.org/wp-content/uploads/2023/12/RAF-2.0-Final-version.pdf
[19] Přizpůsobení termínu pro AAI doménu, viz (anglicky) https://en.wikipedia.org/wiki/Provenance

1.4 Autentizace

Autentizace uživatele (angl. *user authentication*) je proces ověření proklamované digitální identity uživatele.[20]

Přihlášení uživatele (angl. *user login*) je proces, ve kterém na autentizaci navazuje samotný přístup do softwarového systému, resp. uživatelského účtu v tomto systému.

Vícefázové ověření (angl. *multi-factor authentication*, **MFA**) je bezpečnostní proces, kterým se uživatel přihlašuje k účtu, softwarové aplikaci či službě s použitím dvou nebo více faktorů. Faktory spadají do tří kategorií: něco, co uživatel zná (např. heslo, PIN); něco, co uživatel má (např. chytrý telefon, čipovou kartu); anebo něco, co uživatel je (např. geometrie obličeje, otisk prstu). [21]

Jednotné přihlášení (angl. *single sign-on*, **SSO**) je mechanismus, který uživateli umožňuje autentizovat se jednou a následně přistupovat k více poskytovatelům služeb po dobu relace. Analogicky existuje také **jednotné odhlášení** (angl. *single logout*, **SLO**), mechanismus, který uživateli umožňuje hromadně ukončit aktuální relace. [22]

Relace (angl. *session*) je termín, který v kontextu AAI označuje jednak dobu mezi přihlášením a odhlášením uživatele (přičemž odhlášení může být manuální, nebo jej může vynutit systém po uplynutí stanovené lhůty), jednak technické řešení relace. Po dobu platnosti relace se uživatel nemusí v daném systému znovu autentizovat. [23]

[20] (anglicky) https://en.wikipedia.org/wiki/Authentication
[21] (anglicky) https://en.wikipedia.org/wiki/Multi-factor_authentication
[22] (anglicky) https://en.wikipedia.org/wiki/Single_sign-on
[23] (anglicky) https://en.wikipedia.org/wiki/Session_(computer_science)

1.5 Řízení přístupu

Autorizace (angl. *authorization*) je proces tvorby autorizačních pravidel a přidělování oprávnění na základě těchto pravidel. [24]

Řízení přístupu (angl. *access control*) je proces vyhodnocování autorizačních pravidel a kontroly oprávnění. [25]

Řízení přístupu na základě rolí (angl. *role-based access control*, **RBAC**) je varianta řízení přístupu, ve které jsou autorizační pravidla ve tvaru subjekt–role–operace–objekt a přidělení oprávnění spočívá v přiřazení role subjektu. Subjektu je povoleno vykonat operaci na objektu, pokud existuje pravidlo s odpovídající kombinací entit. [26]

Řízení přístupu na základě atributů (angl. *attribute-based access control*, **ABAC**) je varianta řízení přístupu, ve které jsou autorizační pravidla ve tvaru atributy subjektu–operace–objektu–kontextu a přidělení oprávnění spočívá ve vytvoření nového pravidla. Subjektu je povoleno vykonat operaci na objektu, pokud existuje pravidlo s odpovídající kombinací atributů. [27]

Policy enforcement point (**PEP**), ***policy decision point*** (**PDP**), ***policy administration point*** (**PAP**) a ***policy information point*** (**PIP**) (nepřekládáme) jsou čtyři funkční body, které zabezpečují řízení přístupu v distribuovaných prostředích.[28] Jejich definice jsou v sekci 4.1.2.

[24] (anglicky) https://en.wikipedia.org/wiki/Authorization
[25] (anglicky) https://en.wikipedia.org/wiki/Access_control
[26] (anglicky) https://en.wikipedia.org/wiki/Role-based_access_control
[27] (anglicky) https://en.wikipedia.org/wiki/Attribute-based_access_control
[28] (anglicky) doi.org/10.6028/NIST.SP.800-162

1.6 Ostatní

Auditing (angl. *auditing*) je proces zkoumání dat z logování pro zajištění compliance, vyšetření neobvyklého chování nebo identifikaci přetížených míst v systémech. [29]

Citlivá data (angl. *sensitive data*, **SD**) jsou taková, kde manipulace s nimi podléhá specifickým zákazům, nařízením, normám nebo jsou jinak smluvně chráněna.

Compliance (nepřekládáme) je soulad s předpisy, pravidly, požadavky atd. [30]

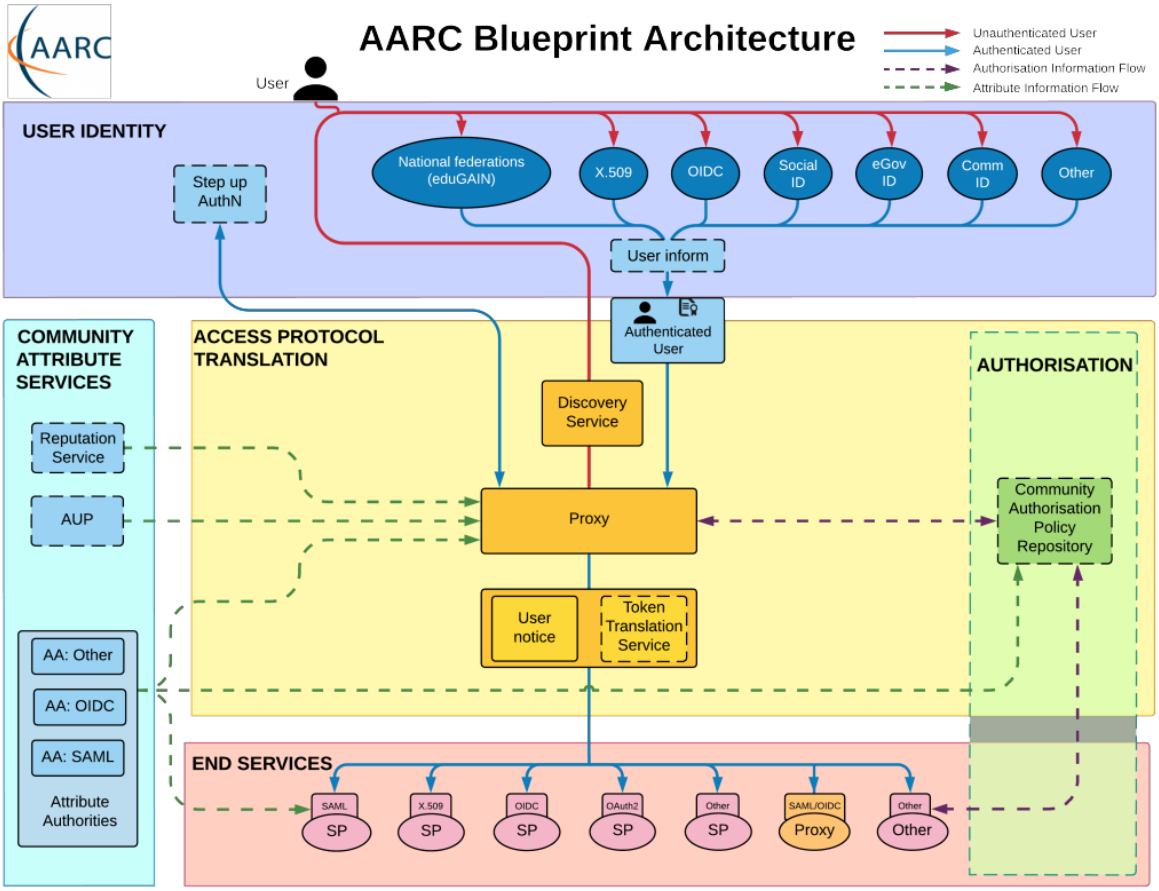
Logování (angl. *accounting*) je proces sbírání dat o tom kdo, co, kde, kdy, proč atp. pro účely auditingu. [31]

Osobní údaje (angl. *personally identifiable information*, PII) jsou informace umožňující přímo nebo nepřímo ztotožnit fyzickou osobu. [32]

[29] Přizpůsobení termínu pro AAI doménu, viz (anglicky) https://en.wikipedia.org/wiki/Audit
[30] https://events.eosc.cz/event/250/attachments/187/377/Prezentace.pdf (s. 26-39)
[31] Přizpůsobení termínu pro AAI doménu, viz (anglicky) https://en.wikipedia.org/wiki/Accounting
[32] (anglicky) https://en.wikipedia.org/wiki/Personal_data

2 Obecné principy

Architektura AAI pro NRP vychází z dokumentů Charta IPS EOSC CZ[33], Studie proveditelnosti NRP[34], Základní obsah projektu NRP[35], standardů mezinárodní inciativy AARC[36] (zejména AARC *Blueprint Architecture*[37]), standardů skupiny REFEDS[38] a historických zkušeností s budováním a provozem AAI pro výzkumné infrastruktury (např. LS AAI[39], e-INFRA CZ AAI[40]).



Obrázek 4: Vrstvy komponent v AARC Blueprint Architecture [41]

[33] https://www.eosc.cz/media/3582629/charta-projektu-ips-eosc-cz.pdf
[34] (odkaz přístupný pouze registrovaným řešitelům projektu NRP) https://researchinfracz.sharepoint.com/:b:/r/sites/NRP/Sdilene%20dokumenty/General/Studie%20proveditelnosti/NRP_Studie_proveditelnosti.pdf
[35] (odkaz ke stažení) https://www.eosc.cz/media/3713976/nrp_zakladni_obsah_projektu_2024.pdf
[36] (anglicky) https://aarc-community.org/
[37] (anglicky) doi.org/10.5281/zenodo.3672785
[38] (anglicky) https://refeds.org/
[39] (anglicky) https://lifescience-ri.eu/ls-login.html
[40] (anglicky) https://docs.e-infra.cz/account/
[41] Zdroj: AARC *Blueprint architecture*, str. 5 (anglicky) doi.org/10.5281/zenodo.3672785

2.1 Struktura EOSC CZ AAI

EOSC CZ AAI má dvě složky: technickou a procesní.

Technicky je EOSC CZ AAI postavená na open-source softwarovém řešení Perun AAI. To se skládá ze dvou hlavních komponent: IdM a ProxyIdP. Obě jsou modulární softwarové aplikace složené z mikro-komponent, které se dají konfigurovat, vyměňovat anebo rozšiřovat. Součástí Perun AAI jsou pak ještě další, vedlejší komponenty, které do něj doplňují další funkcionalitu. Díky tomu lze celkové řešení přizpůsobit konkrétnímu prostředí a jeho požadavkům.

Poznámka: *Konkrétní softwarové aplikace či knihovny, které se v Perun AAI používají, se mohou a budou v průběhu projektu NRP měnit. Na architekturu AAI v NRP nebo její fungování by to nemělo mít žádný zásadní dopad – rozhraní zůstanou v maximální míře zachována.*

Procesně je EOSC CZ AAI postavena na požadavcích české legislativy, na pravidlech sdružení CESNET[42] (provozovatel EOSC CZ AAI), na provozních podmínkách EOSC CZ AAI[43] a na technické a uživatelské dokumentaci EOSC CZ AAI. Dohromady se tím stanovují práva, povinnosti, možnosti a pracovní postupy správců AAI, správců entit vedených v AAI a koncových uživatelů (ale jenom ve vztahu k AAI).

Poznámka: *Přesné znění zákonů, smluv a pravidel se může a bude v průběhu projektu NRP měnit. Dopad změn na architekturu AAI v NRP nebo její fungování nelze úplně předvídat.*

Upozornění: *Požadujeme, aby měl každý uživatel v EOSC CZ AAI jenom jeden uživatelský účet, bez ohledu na jeho příslušnost (afiliaci) k jedné nebo více organizacím (naraz i v čase), aby nedocházelo k problémům při autorizaci uživatele a řízení přístupu. Toho jde nejlépe dosáhnout, když si uživatelé zakládají účty sami, registrací. Odmítáme proto automatické vytváření účtů v AAI (nikoliv autorizačních pravidel!), např. synchronizací z externích systémů.*

2.2 Provozní parametry EOSC CZ AAI

EOSC CZ AAI běží ve virtualizační infrastruktuře sdružení CESNET[44]. Předpokládaná dostupnost je 99 % času. V případě problémů je považována za kritickou službu a obnovuje se mezi prvními. Její data se zálohují každý den.

Provozovatel EOSC CZ AAI má zavedený systém řízení bezpečnosti informací (ISMS), je držitelem certifikace dle ČSN EN ISO/IEC 27001:2014 a bude regulován v režimu vyšších povinností dle nového zákona o kybernetické bezpečnosti[45]. Osobní údaje uživatelů EOSC CZ AAI jsou zpracovávány výlučně na území České republiky.

Poznámka: *Provozovatel EOSC CZ AAI vynakládá veškeré možné úsilí pro dosažení těchto parametrů, ale bez konkrétních záruk.*

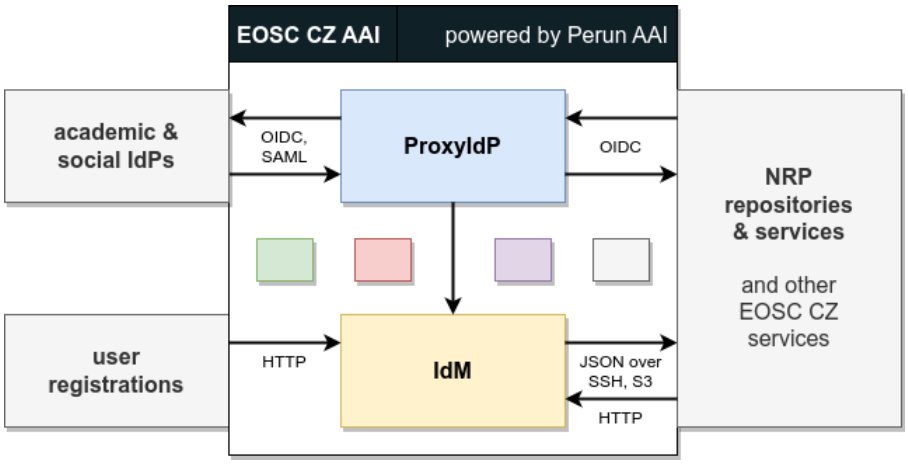
[42] https://www.cesnet.cz/pravni-informace#dokumenty-sdruzeni-230
[43] (odkaz ke stažení) https://e-infra.cz/aai-podminky
[44] https://www.cesnet.cz/sluzby/vypocty-2/virtualni-servery-17
[45] https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti

2.3 Integrace repozitářů a služeb NRP

R/S NRP musí být dvojitě připojeny k EOSC CZ AAI pro zabezpečení řádné autentizace a autorizace uživatelů NRP. Připojením k ProxyIdP komponentě se zabezpečí SSO a umožní sběr a aktualizaci atributů potřebných pro řízení přístupu. Připojením k IdM komponentě se zabezpečí *just-in-case* provisioning a deprovisioning.

Poznámka: *Pokud to implementace R/S NRP umožňuje, můžou být připojené i k dalším IdP či AAI a můžou obsahovat i čistě lokální účty.*

Technicky se R/S NRP připojí k ProxyIdP komponentě protokolem OIDC[46,47] a k IdM komponentě JSON konektorem[48] ve směru do R/S NRP a přes RPC API[49] ve směru do AAI.



Obrázek 5: EOSC CZ AAI a její integrace v kontextu NRP

Speciálně pro repozitáře NRP (nikoliv služby) existují tři situační varianty připojení:

1. V první variantě se k EOSC CZ AAI připojuje *nový* repozitář postavený na základním repozitářovém systému provozovaný v prostředí NRP. Vývojáři repozitářového systému musí připojení repozitáře automatizovat jako součást jeho postavení. Správci AAI poskytnou nutnou podporu a zabezpečí doplnění chybějící funkcionality do systému Perun AAI.
2. Ve druhé variantě se k EOSC CZ AAI připojuje *existující* repozitář postavený na základním repozitářovém systému provozovaný v prostředí NRP. Vývojáři repozitářového systému musí oproti první variantě zabezpečit navíc i automatickou migraci existujících účtů tak, aby došlo k jejich propojení s účty v AAI[50]. Správci AAI poskytnou nutnou podporu a zabezpečí doplnění chybějící funkcionality v systému Perun AAI.
3. Ve třetí variantě se k EOSC CZ AAI připojuje nový či existující repozitář postavený na alternativním repozitářovém systému nebo provozovaný v alternativním prostředí. Připojení musí zařídit vývojáři repozitářového systému anebo správci repozitáře. Správci AAI zabezpečí standardní rozhraní a související technickou dokumentaci.

[46] (anglicky) https://openid.net/specs/openid-connect-core-1_0-final.html
[47] Protokol OIDC je potřeba kvůli efektivní implementaci integrace repozitářů a výpočetních *workflows*.
[48] (anglicky) https://github.com/CESNET/perun-services/blob/main/docs/services/generic_json_gen.md
[49] (anglicky) https://perun-aai.org/documentation/technical-documentation/rpc-api/
[50] Jinak řečeno, uživatel repozitáře nesmí po jeho připojení k EOSC CZ AAI ztratit stávající oprávnění.

2.4 Integrace poskytovatelů identit

EOSC CZ AAI je připojená k české akademické federaci identit eduID[51], celosvětové akademické inter-federaci identit eduGAIN[52] a několika vybraným sociálním IdP: ORCID[53], Microsoft, Google, Apple a další.[54] Tím je přístupná jak českým, tak zahraničním akademikům i partnerům mimo akademické prostředí.

V plánech rozvoje EOSC CZ AAI je připojení k alespoň jednomu prostředku pro ověření totožnosti uživatele (např. eID[55]) a zapojení se do evropské EOSC AAI federace[56] jako jeden z uzlů.

Poznámka: *Pokud by některým R/S NRP chyběl nějaký potřebný IdP, ať jejich správci či vývojáři kontaktují NRP KA 4.3* [57]*.*

[51] https://www.eduid.cz/cs/index
[52] (anglicky) https://edugain.org/
[53] (anglicky) https://orcid.org/
[54] Seznam IdP ve federacích identit či sociálních IdP se může v průběhu projektu NRP i poté měnit.
[55] eID je digitální prostředek ověření totožnosti uživatele dle evropské regulace eIDAS:
https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910
V ČR je eID implementované jako Identita Občana:
https://www.identita.gov.cz/
[56] (anglicky) doi.org/10.5281/zenodo.10379292
[57] nrp-ka4-3-data-access@eosc.cz

3 Autentizační infrastruktura

3.1 Registrace uživatele

Registrace uživatele je mechanismus v systému Perun AAI pro vytváření uživatelských účtů, vznik členství uživatele ve VO a skupinách, sběr uživatelských atributů a informování uživatele.

Každý uživatel, který chce přistupovat k R/S NRP, se prvně musí registrovat do EOSC CZ AAI. Tím získá jednotný AAI identifikátor[58], oprávnění pro přístup k R/S NRP (kapitola 4) a během registrace i možnost obeznámit se s dokumenty compliance[59].

Z pohledu uživatele: *V prvním kroku přijme personalizovanou pozvánku nebo otevře veřejný odkaz na registraci. Ve druhém kroku se přihlásí (sekce 3.3) do registrační aplikace EOSC CZ AAI. Ve třetím kroku vyplní jeden formulář (žádost o registraci), ve kterém taky najde odkazy na dokumenty compliance, které musí znát. V posledním kroku čeká na schválení registrace, které může být automatické nebo manuální.*

Poznámka: *Správci repozitáře musí pro správné nastavení registračních procesů předem dodat potřebné informace. Povinné jsou jméno a krátký popis R/S NRP a sada odkazů na dokumenty compliance spojené s AAI (např. provozní podmínky). Nepovinná jsou grafická značka R/S NRP a seznam nadstandardních atributů nutných pro řízení přístupu.*

Informace o vzniku členství (a implicitně o nabytí souvisejících oprávněních) se do R/S NRP předá přes domluvená rozhraní (sekce 2.3) jednak při nejbližším přihlášení (sekce 3.3), jednak okamžitě přes provisioning (sekce 3.4). R/S NRP musí tuto informaci okamžitě reflektovat v řízení přístupu (sekce 4.2.4).

3.1.1 Exspirace členství

Exspirace členství je mechanismus v systému Perun AAI pro ukončení členství uživatele ve VO nebo skupině. Cílem je zabezpečit, aby si uživatel neponechával nepotřebná oprávnění, které mu vyplývají z členství ve VO nebo skupině (sekce 4.2.3).

Exspirace má dvě varianty:

1. První varianta je manuální. Exspiraci musí provést správce příslušné VO nebo skupiny co nejdříve poté, co rozhodl o odebrání přístupu uživateli.
2. Druhá varianta je automatická. Exspiraci provede systém v předem stanovené datum. Slouží jako záložní mechanismus, když správce VO nebo skupiny zapomene provést manuální exspiraci.

Poznámka: *Správci R/S NRP musí nastavit automatickou exspiraci ve svých VO a skupinách předtím, než se do nich dostane první uživatel. Změna nastavení se totiž nevztahuje na stávající členy – jejich datum exspirace musí upravit zvlášť.*

Informace o konci členství (a implicitně o pozbytí souvisejících oprávnění) se do R/S NRP předá přes domluvená rozhraní (sekce 2.3) jednak při nejbližším přihlášení (sekce 3.3), jednak okamžitě přes deprovisioning (sekce 3.4.1). R/S NRP musí tuto informaci okamžitě reflektovat v řízení přístupu (kapitola 4).

---

[58] Identifikátor vydávaný EOSC CZ AAI je v jejím rámci unikátní, permanentní a nepřenosný. Je určen k jednoznačné identifikaci uživatele v připojených SP. Avšak pozor, po smazání účtu se již nesmí znovu použít, a to ani pro stejného uživatele.

[59] Tj. pravidla sdružení CESNET a provozní podmínky EOSC CZ AAI (sekce 2.1).

3.1.2 Prodloužení členství

Prodloužení členství je mechanismus v systému Perun AAI, který umožňuje včas předejít automatické exspiraci, pokud uživatel nadále potřebuje oprávnění, které mu vyplývají z členství ve VO nebo skupině (sekce 4.2.3).

Z pohledu uživatele: *V prvním kroku otevře odkaz v notifikačním emailu upozorňujícím na blížící se exspiraci členství. Ve druhém kroku se přihlásí (sekce 3.3) do registrační aplikace EOSC CZ AAI. Ve třetím kroku vyplní formulář (žádost o prodloužení). A v posledním kroku čeká na schválení žádosti, které může být automatické nebo manuální.*

3.2 Správa uživatelského profilu

Každý uživatel si může spravovat svůj uživatelský profil[60] v EOSC CZ AAI. Obvykle si potřebuje aktualizovat svůj preferovaný email, propojit svoje digitální identity (sekce 3.2.1) anebo přenastavit MFA (sekce 3.3.1).

3.2.1 Propojení digitálních identit uživatele

Každý uživatel EOSC CZ AAI si může propojit všechny nebo některé svoje digitální identity, jejichž IdP jsou připojeni k EOSC CZ AAI (sekce 2.4). Primární výhoda tohoto propojení je sjednocení oprávnění uživatele bez ohledu na jeho identitu použitou pro autentizaci. Vedlejší výhoda je zachování přístupu k EOSC CZ AAI účtu, i když uživatel ztratí přístup k jedné ze svých propojených identit.

Z pohledu uživatele: *V prvním kroku se uživatel přihlásí (sekce 3.3) do svého uživatelského profilu v EOSC CZ AAI (sekce 3.2). Ve druhém kroku spustí samotný proces propojení. Ve třetím kroku si vybere digitální identitu, kterou chce propojit s těmi stávajícími. A v posledním kroku se přes odpovídající IdP autentizuje digitální identitou, kterou vybral v předešlém kroku.*

Poznámka: *Různá IdP nabízí různou sílu autentizace, R/S NRP proto mohou požadovat minimální úroveň AAL (sekce 3.5).*[61] *EOSC CZ AAI pak zaručí, že se uživatel autentizuje přes IdP, které tyto podmínky splňuje.*

3.3 Přihlášení uživatele

Přihlášení uživatele je nutnou podmínkou pro přístup k zdrojům R/S NRP, s výjimkou pro čtení otevřených dat a metadat. Aby se ale uživatel nemusel přihlašovat jednotlivě do jednotlivých R/S NRP, EOSC CZ AAI poskytuje mechanismus SSO.

EOSC CZ AAI při přihlášení do R/S NRP posílá atributy dle standardů REFEDS[62] a AARC[63]. V tomto případě se vlastně jedná o *just-in-time* provisioning a deprovisioning uživatele.

[60] (česky nebo anglicky, po přihlášení) https://profile.e-infra.cz/
[61] R/S NRP toho můžou ohledně *identity assurance* požadovat víc, viz sekci 4.2.5.
[62] (anglicky) https://wiki.refeds.org/
[63] (anglicky) https://aarc-community.org/

Poznámka: *Pokud by většině R/S NRP při přihlašování nějaký atribut chyběl, ať jejich správci či vývojáři kontaktují NRP KA 4.3 [64].*

Z pohledu uživatele: *V nultém kroku se uživatel pokusí přistoupit na R/S NRP, který jej jako neautentizovaného uživatele přesměruje do EOSC CZ AAI. V prvním kroku si vybere IdP (tj. digitální identitu), kterým se chce autentizovat (zde si obvykle zvolí akademickou identitu dle afiliace anebo oblíbenou sociální identitu). Ve druhém kroku se autentizuje (obvykle jménem a heslem). A v posledním kroku jej EOSC CZ AAI přesměruje zpět na R/S NRP.*

Po prvním přihlášení už není potřeba se znovu autentizovat. Systémy si dle potřeby vymění informace, doplní chybějící relace a uživatel může po (přinejhorším) několika přesměrováních pokračovat ve své práci dál, dokud se neodhlásí nebo dokud mu nevyprší relace jak v EOSC CZ AAI, tak v jeho IdP.

Poznámka: *EOSC CZ AAI je nastavená tak, aby si pamatovala poslední IdP, které si uživatel vybral. Zároveň R/S NRP mohou indikovat filtrování seznamu IdP anebo předvyplněné IdP.*

3.3.1 Vícefázové ověření

MFA zvyšuje zabezpečení uživatelského účtu, protože chrání proti útokům, které jinak můžou uspět vůči jednotlivým autentizačním faktorům (např. krádež nebo uhodnutí hesla, odcizení nebo zneužití čipové karty, *phishing* atp.). Proto MFA doporučujeme nejen pro přístup k R/S NRP, přestože snižuje uživatelský komfort. [65]

Poznámka: *EOSC CZ AAI v současnosti podporuje tyto faktory: WebAuthn[66] (doporučujeme), TOTP[67], a záložní klíče na jedno použití.*

Když uživatelé musí či chtějí MFA používat, tak jej musí nastavit a provádět v IdP. Pouze když žádné jejich IdP nepodporuje MFA anebo *Multi-Factor Authentication profile*[68], tak uživatelé musí MFA nastavit a provádět v EOSC CZ AAI.

Z pohledu uživatele: *V nultém kroku si uživatel nastaví MFA v EOSC CZ AAI (sekce 3.2), protože jej jeho IdP jej neumí. Konkrétní nastavení je závislé na faktorech, které chce využívat. V prvním kroku se v IdP standardně autentizuje (sekce 3.3). A ve druhém (a posledním) kroku jej EOSC CZ AAI během přesměrování do R/S NRP vybídne k provedení MFA. Po dobu trvání relace již není potřeba MFA opakovat (pokud o to některý R/S NRP explicitně nezažádá).*

3.3.2 Relace

Po přihlášení uživatele mechanismem SSO vznikají relace na třech úrovních: v IdP, v EOSC CZ AAI a v R/S NRP. Každá relace je spravována odpovídajícím systémem – v současnosti není úkolem EOSC CZ AAI řídit relace vytvořené jinde než v rámci EOSC CZ AAI.

Nejdůležitější vlastností relace je doba platnosti: příliš krátká relace není uživatelsky přívětivá (uživatel se musí často autentizovat), příliš dlouhá relace je zas méně bezpečná (narůstá riziko

---

[64] nrp-ka4-3-data-access@eosc.cz

[65] V roce 2025 navíc vstoupí v platnost nový zákon o kybernetické bezpečnosti implementující evropskou směrnici NIS2, který pro regulované subjekty zavádí povinné MFA. Compliance s legislativou zabezpečí EOSC CZ AAI.

[66] (anglicky) https://w3c.github.io/webauthn/
Laicky oskenování prstu či obličeje v chytrém telefonu, použití YubiKey tokenu apod.

[67] (anglicky) https://en.wikipedia.org/wiki/Time-based_one-time_password
Laicky opisování pravidelně se měnícího číselného kódu z telefonu.

[68] (anglicky) https://refeds.org/profile/mfa a https://wiki.refeds.org/display/PRO/MFA+Profile+FAQ

únosu relace). Tato zpráva žádná doporučení pro R/S NRP nevydává[69], jejich správci si sami volí optimální dobu platnosti.

3.3.3 Odhlášení uživatele

Uživatel se může přes svůj uživatelský profil v EOSC CZ AAI (sekce 3.2) odhlásit. Ukončuje tím ale jenom relaci, kterou vytvořila EOSC CZ AAI, ostatní zůstávají platné – Perun AAI v současnosti nemá implementovaný mechanismus SLO[70], ale ten je v plánech jeho rozvoje.

3.4 Provisioning uživatele

Just-in-case provisioning je mechanismus v Perun AAI, který se používá pro:

- zřízení lokálního uživatelského účtu v řízeném systému, ke kterému se nelze přihlásit přes SSO (např. kvůli povolení přístupu do Unixového účtu),
- zřízení lokálního uživatelského účtu před prvním přihlášením do řízeného systému přes SSO (např. kvůli povolení přístupu do repozitáře NRP přes API),
- aktualizaci uživatelského účtu v řízeném systému dřív, než se uživatel znovu přihlásí přes SSO (např. kvůli aktualizaci přístupu pro asynchronní proces).

Technicky EOSC CZ AAI monitoruje změny ve svých datech, identifikuje dotčené R/S NRP a provádí asynchronní propagaci (odesílání) aktuálního stavu[71] relevantní podmnožiny dat. Odeslaná data se ukládají JSON souboru, který slouží jako mezi-úložiště a rozhraní mezi AAI a R/S NRP (sekce 2.3). R/S NRP musí tyto data v co nejkratším čase zpracovat a upravit podle nich lokální uživatelské účty.

3.4.1 Deprovisioning uživatele

Just-in-case deprovisioning je mechanismus v Perun AAI, který se používá pro co nejrychlejší odebrání oprávnění uživateli v řízeném systému. Technicky používá stejné řešení jako provisioning (sekce 3.4).

3.5 Identity assurance

R/S NRP mohou požadovat *identity assurance* vyšší úrovně pro autorizaci uživatele (např. pro přístup k citlivým datům) nebo pro audit (např. během řešení bezpečnostního incidentu). Informaci o dosažené úrovni *identity assurance* získá z EOSC CZ AAI během přihlášení.[72]

Pro určení dosažené úrovně *identity assurance* je potřeba jednotlivě prozkoumat její tři složky:

---

[69] Jen pro kontext, platnost relace EOSC CZ AAI je 24 hodin od přihlášení.

[70] SLO podporují protokoly OIDC i SAML:
(anglicky) https://openid.net/specs/openid-connect-frontchannel-1_0.html
(anglicky) https://openid.net/specs/openid-connect-backchannel-1_0.html
(anglicky) https://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/saml-async-slo-v1.0.html

[71] Perun AAI v současnosti neumí dělat rozdílové operace a posílá aktuální stav dat. Nicméně je pro tento přístup optimalizovaná a výkonnostně většinou stačí. Do budoucna se tento přístup může změnit, konkrétní plán ale zatím není.

[72] (anglicky) https://wiki.refeds.org/display/STAN/eduPerson+2020-01#eduPerson202001-eduPersonAssurance

- *identity assurance level* (IAL) popisuje důvěru ve způsob ověření totožnosti,
- *authentication assurance level* (AAL) popisuje důvěru v sílu autentizace,
- *federation assurance level* (FAL) popisuje důvěru v zabezpečení federace.

Každá z těchto složek má tři úrovně: nízkou, značnou a vysokou.[73] EOSC CZ AAI aktuálně nabízí úroveň nízká, pracuje se na podpoře pro úroveň značná (mimo jiné integrací eID[74]).

[73] Definice se různí, za autoritativní zdroj považujeme:
(anglicky) doi.org/10.6028/NIST.SP.800-63-3 (sekce 5.2)
[74] eID je digitální prostředek ověření totožnosti uživatele dle evropské regulace eIDAS:
https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910
V ČR je eID implementované jako Identita Občana:
https://www.identita.gov.cz/

4 Autorizační infrastruktura

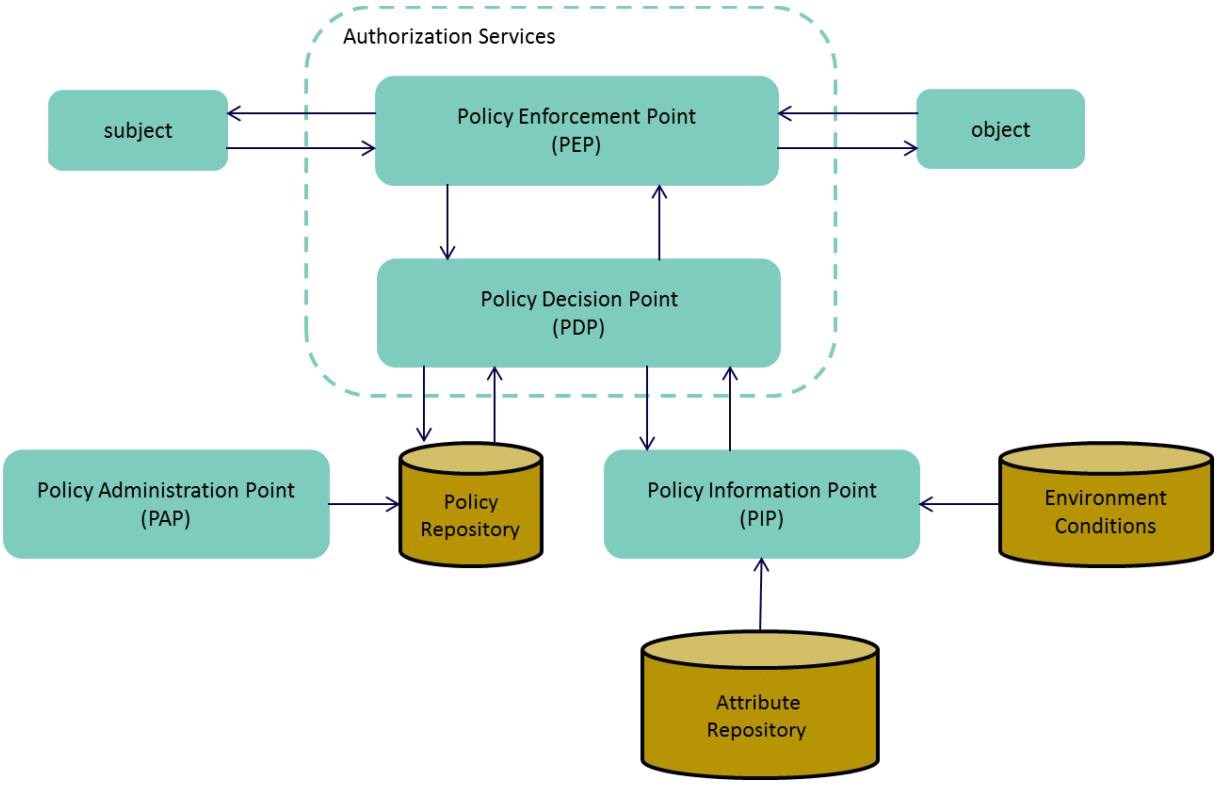
4.1 Teoretické základy

4.1.1 Subjekty v řízení přístupu

Subjektem v autorizačních pravidlech obvykle bývá digitální identita; oprávnění se přidělují jí. Aby bylo možné tvrdit, že se oprávnění přidělilo konkrétnímu uživateli, musí tato digitální identita mít značnou nebo vysokou *identity assurance* (sekce 3.5). Je potřeba počítat také s tím, že subjektem může být také servisní účet v AAI (sekce 5.3), jehož oprávnění nepřímo nabývají všichni jeho správci.

4.1.2 Architektura řízení přístupu

Řízení přístupu zabezpečují v distribuovaných prostředích čtyři funkční body: *policy enforcement point* (PEP), *policy definition point* (PDP), *policy administration point* (PAP) a *policy information point* (PIP).[75]



Obrázek 6: Ilustrace funkčních bodů v distribuovaném řízení přístupu dle ABAC [76]

- **PEP** odpovídá za vynucení rozhodnutí z PDP o schválení či zamítnutí přístupu. PEP je vždy součástí implementace R/S NRP.

[75] (anglicky) doi.org/10.6028/NIST.SP.800-162
Tato publikace definuje řízení přístupu na základě atributů (angl. attribute-based access control, ABAC). Sekce 2.4.3 (obr. č. 5) v ní popisuje mechanismus pro distribuované řízení přístupu a "funkční body" potřebné k jeho implementaci. Tento mechanismus lze aplikovat na problematiku řízení přístupu v NRP, komponenty ekosystému NRP lze mapovat na "funkční body" popsané v publikaci a tím ilustrovat jejich část odpovědnosti v různých modelech řízení přístupu.
[76] (ibid.)

- **PDP** odpovídá za vyhodnocení autorizačních pravidel z jednoho nebo více PAP dle informací z jednoho nebo více PIP a vydání rozhodnutí o schválení nebo zamítnutí přístupu. PDP je buď součástí implementace R/S NRP, anebo je to specializovaná komponenta úzce s ním propojená.
- **PAP** odpovídá za správu autorizačních pravidel. V ekosystému může být jeden, nebo jich může být více. PAP může být součástí implementace R/S NRP, může to být EOSC CZ AAI, anebo samostatný systém, např. OPA[77].
- **PIP** odpovídá za dodání informací o subjektu, operaci, objektu či kontextu. V ekosystému může být jeden, nebo jich může být více. PIP může být součástí implementace R/S NRP, může to být EOSC CZ AAI, anebo samostatný systém, např. REMS[78].

Když se v průběhu projektu NRP najdou vhodné příležitosti pro centralizaci řešení, tak se mapování funkčních bodů na komponenty ekosystému NRP může změnit; např. EOSC CZ AAI může převzít větší díl odpovědnosti za řízení přístupu.

4.2 Iniciální model řízení přístupu

V iniciálním modelu řízení přístupu R/S NRP interně implementují RBAC. EOSC CZ AAI je jen autoritativním zdrojem pro přiřazení rolí uživatelům.

4.2.1 Subjekty a objekty

Subjektem řízení přístupu je lokální uživatelský účet v R/S NRP spojený s jednou EOSC CZ AAI identitou a přes ni s jednou nebo více IdP identitami[79].

Objektem řízení přístupu je v případě repozitáře NRP množina datových sad, jejíž velikost závisí na granularitě rolí.[80] Co je objektem ve službě NRP vždy závisí na konkrétním systému.

4.2.2 Funkční body

R/S NRP plní funkci:

- PEP: reálně povoluje/zakazuje provedení operace na základě svého rozhodnutí
- PDP: sám rozhoduje, zda se operace smí provést na základě svých informací
- PAP: definuje seznam rolí a pro každou z nich její oprávnění pro kategorie objektů
- PIP: drží informace o účtech a jejich rolích, objektech a jejich kategoriích, propojení účtů s digitálními identitami v AAI

EOSC CZ AAI plní funkci PIP: spravuje informace o přiřazení rolí k digitálním identitám v AAI.

4.2.3 Model dat v AAI

R/S NRP jsou v EOSC CZ AAI reprezentované entitou *Facility* a množina uživatelů R/S NRP je reprezentovaná entitou *VO*. Správce R/S NRP je v AAI správcem těchto dvou typů entit.

Komunity a role uvnitř R/S NRP jsou v EOSC CZ AAI reprezentované párem entit *Group* (skupina) a *Resource* (zdroj). Na základě členství uživatele ve VO a skupinách v EOSC CZ AAI jsou pak jeho uživatelskému účtu v R/S NRP přiřazeny příslušné role.

---

[77] (anglicky) https://www.openpolicyagent.org/
[78] (anglicky) https://github.com/CSCfi/rems
[79] Účet je s uživatelem spojený jenom v případě, že je *identity assurance* alespoň značná.
[80] Srovnej role: správce repozitáře, datový kurátor komunity, vlastník datové sady.

4.2.4 Integrace

EOSC CZ AAI pak předává informace o přiřazení rolí k AAI identitám během přihlášení uživatele ve formě *resource capabilities*[81] a při změnách v těchto datech přes provisioning do JSON souboru. *Postprocessing script* na straně R/S NRP pak tento soubor musí včas zpracovat a aktualizovat účty a jejich role v R/S NRP přes REST API.

4.2.5 Citlivá data

V případě, že R/S NRP pracují s citlivými daty, *identity assurance* subjektu musí být alespoň značná (sekce 3.5). Tím se zajistí, že lokální uživatelský účet v R/S NRP (subjekt řízení přístupu) lze přes AAI identitu a přes IdP identitu důvěryhodně propojit s uživatelem (fyzickou osobou).

Poznámka: *dosud si lidi pracující s citlivými daty vystačili s:*

- *důvěrou v akademické IdP, že defacto ověřují totožnost na úrovni IAL2,*
- *důvěrou v příznak, že IdP provedlo MFA na úrovni AAL2,*
- *důvěrou v komunitní AAI na úrovni FAL1,*
- *řízením přístupu na úrovni projektu (řídí si jej sám* principal investigator).

[81] (anglicky) doi.org/10.5281/zenodo.3701348

5 Podpůrné funkce

5.1 Uživatelská podpora

Uživatelská podpora pro EOSC CZ AAI je poskytována ve čtyřech úrovních[82]:

1. Úroveň 0: uživatelská dokumentace
2. Úroveň 1: obecný helpdesk provozovatele AAI
3. Úroveň 2: odborný helpdesk oddělení AAI
4. Úroveň 3: konzultanti EOSC CZ AAI

5.1.1 Hlášení bezpečnostních incidentů

Správci R/S NRP nebo koncoví uživatelé musí v případě bezpečnostního incidentu či podezření na něj postupovat dle návodu[83] týmu CESNET-CERTS[84] a bez prodlení poslat hlášení na emailovou adresu: certs@cesnet.cz

5.2 Logování a auditing

V EOSC CZ AAI loguje každá její komponenta, přičemž nejdůležitější data sbírají ty dvě hlavní: ProxyIdP a IdM. První loguje použité IdP, z něj získané uživatelské atributy, cílové SP a do něj předané uživatelské atributy. Druhá loguje uživatelské akce a entity, atributy a vazby, kterých se akce dotkly. Logy se drží po dobu nezbytně nutnou.[85]

Poznámka: *EOSC CZ AAI nesbírá data pro auditing z připojených systémů.*

V současné verzi EOSC CZ AAI provádí auditing její správci manuálním projitím logů. Třetím stranám logy nejsou přímo přístupné.

5.3 Servisní účet v AAI

Servisní účet v AAI se používá pro volání Perun RPC API[86], když R/S NRP potřebuje zapsat data do EOSC CZ AAI (sekce 2.3).

Provozní podmínky EOSC CZ AAI[87] vyžadují, aby měl každý servisní účet v AAI alespoň jednoho vlastníka, který za něj odpovídá. Rovněž popisují životní cyklus servisního účtu.

[82] https://cs.wikipedia.org/wiki/Technick%C3%A1_podpora
[83] https://csirt.cesnet.cz/cs/incident_report
[84] https://csirt.cesnet.cz/cs/index
[85] https://www.cesnet.cz/pravni-informace#doba-uchovavani-osobnich-udaju-211
[86] (anglicky) https://perun-aai.org/documentation/technical-documentation/rpc-api/
[87] (odkaz ke stažení) https://e-infra.cz/aai-podminky

5.4 Lokalizace uživatelských rozhraní

Celé uživatelské rozhraní systému Perun AAI je lokalizované v anglickém jazyku. Uživatelské rozhraní mikro-komponent registrační aplikace (sekce 3.1) a uživatelského profilu (sekce 3.2), které jsou určené běžným koncovým uživatelům, jsou navíc lokalizované i v českém jazyku.