

ELEKTRONIZACE ZDRAVOTNICTVÍ

Registr oprávnění

Účel, funkce a vnější API rozhraní



Projekt Národní centrum elektronického zdravotnictví (registrační číslo
CZ.31.1.01/MV/22_05/0000005)

Verze: 00/00

Platnost nové verze od: 999

Obsah

1	Účel komponenty:	4
1.1	Funkční přínos v rámci systému	4
1.2	Zákonné požadavky, které komponenta naplňuje	4
1.3	Cílové skupiny uživatelů (např. lékaři, pacienti, instituce)	4
1.4	UseCase	4
2	Funkce komponenty:	6
2.1	Přehled hlavních funkcí	6
2.2	Vnitřní logika (např. zpracování dat, ukládání, validace)	7
2.3	Vazby na jiné komponenty	7
3	Vnější rozhraní (API)	8
3.1	Popis poskytovaných služeb (např. REST API, SOAP, jiná)	8
3.2	Formát výměny dat (např. JSON, XML)	8
3.3	Autentizace/autorizace (např. eIDAS, OAuth2, JWT, NIA...)	8
3.4	Popis koncových bodů (endpointů) včetně:	8
3.5	URL	8
3.6	Parametry	9
3.7	Struktura odpovědi	10
3.8	HTTP kódy a chybové stavy	12
4	Testovací scénáře (volitelné)	13
4.1	Přehled testovacích scénářů	13
4.2	Apod.	13
5	Bezpečnostní opatření	14
5.1	Způsob zabezpečení komunikace	14
5.2	Autentizace	14
5.3	Šifrování, auditní logy, role	14
5.4	Apod.	14
6	Provozní požadavky (volitelné)	15
6.1	Nároky na infrastrukturu	15
6.2	Možnosti škálování	15

Seznam zkratek a pojmů

Zkratka	Význam
AIFO	Agendový Identifikátor Fyzické Osoby
JSU	Jednotná Správa Uživatelů
KZR	Kmenové Zdravotnické Registry
KRP	Kmenový Registr Pacientů
KRZP	Kmenový Registr Zdravotních Pracovníků
KRPZS	Kmenový Registr Poskytovatelů Zdravotních Služeb
NPEZ	Narodní Portál Elektronického Zdravotnictví
REZA	Registr Zastupování
RID	Resortní Identifikátor

Účel:

Detailní technicko-funkční dokumentace sloužící architektům systému, programátorům a integračním partnerům.

Rozsah:

5–20 normostran podle rozsahu funkcí komponenty

1 Účel komponenty:

1.1 Funkční přínos v rámci systému

Hlavním účelem Registru oprávnění (RO) je evidovat, ověřovat a poskytovat údaje o oprávněních třetích osob (dále jen „oprávnění“) v oblasti agend a služeb elektronického zdravotnictví, a zajistit tak, že pouze oprávněné osoby mají přístup k odpovídajícím zdravotním údajům (příp. dalším službám EZ) v souladu s právními předpisy a rozhodnutími pacienta.

RO eviduje a administruje oprávnění k využívání služeb elektronického zdravotnictví, resp. k zastupování subjektů. Prostřednictvím systému JSU autorizuje uživatele k nastaveným oprávněním.

RO spravuje implicitní oprávnění k zastupování (vznikající na základě zákona či rozhodnutí soudu) převzatá z REZA, i explicitní oprávnění udělená opravňujícím subjektem. Správcům umožňuje editaci šablon, podle kterých se udělují jednotlivá oprávnění.

1.2 Zákonné požadavky, které komponenta naplňuje

Registr oprávnění implementuje § 32-34 dle novely zákona 325/2021 Sb.:

§ 32 „Registr oprávnění (...) zajišťuje

evidenci pacientem udělených souhlasů třetím osobám a odvolaných souhlasů,

službu ověření přístupu třetích osob ke službám elektronického zdravotnictví na základě souhlasu uděleného pacientem (...)“

§ 34 „Poskytovatel zdravotních služeb je povinen využívat Registr oprávnění pro využití svých informačních systémů umožňujících dálkový přístup pro pacienta.“

1.3 Cílové skupiny uživatelů (např. lékaři, pacienti, instituce)

1.3.1 Pacienti

Používají mikrofrontend NPEZ ke správě oprávnění – poskytnutí, případně odepření oprávnění třetím osobám.

1.3.2 Zdravotničtí pracovníci

Mohou využívat oprávnění získaná od pacienta k jeho zastupování v určitých službách či úkonech EZ.

1.3.3 Poskytovatel zdravotních služeb

Používají mikrofrontend NPEZ ke správě svých zástupců.

1.3.4 Uživatelé systémů eZdrav

Uživatelé systémů eZdrav, kteří se přihlašují pomocí JSU. Prostřednictvím JSU v Access Token a UserInfo získávají autorizaci k zastupování podle udělených oprávnění.

1.4 UseCase

Základní případy užití:

Opravňující osoba

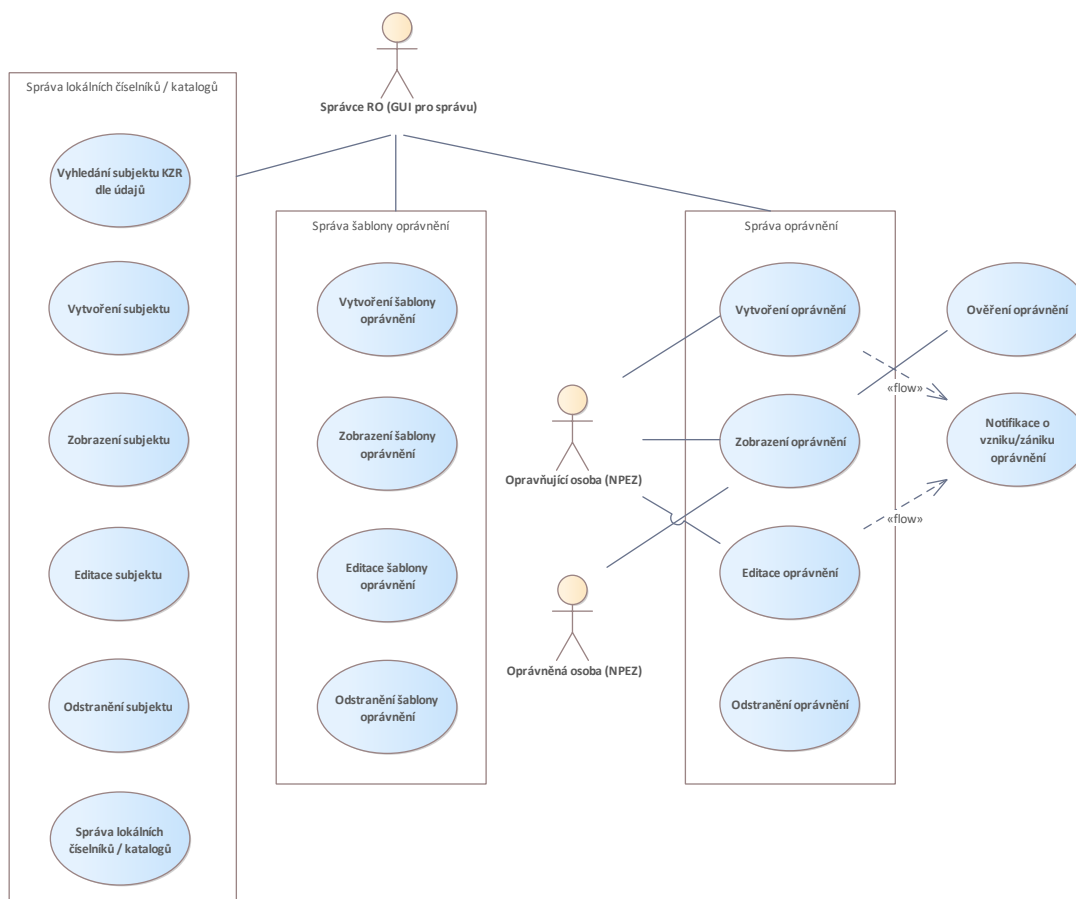
- Vytvoření oprávnění
- Zobrazení oprávnění
- Editace oprávnění

Oprávněná osoba

- Zobrazení oprávnění

Správce systému

- Správa šablon oprávnění
- Správa oprávnění
- Správa lokálních číselníků a katalogů



2 Funkce komponenty:

2.1 Přehled hlavních funkcí

2.1.1 Správa šablon oprávnění

Evidence šablon oprávnění a katalogů potřebných pro definici šablon oprávnění (katalog agend, služeb EZ, nad kterými jsou definovány rozsahy oprávnění).

Šablony určují pravidla, podle kterých je možné oprávnění udělovat.

Registr oprávnění umožňuje administrátorům na backendu (přes administrátorské GUI) tyto šablony oprávnění editovat.

2.1.2 Správa subjektů oprávnění

Evidence opravňujících a oprávněných osob (včetně evidence zástupců).

Reakce na změnu – např. reakce na zrušení oprávnění osoby za zákona (již není jednatel, ukončení poskytování zdravotních nebo sociálních služeb atd.).

2.1.3 Správa oprávnění

Vznik oprávnění je odlišný pro implicitní a explicitní oprávnění. Implicitní oprávnění jsou vytvářena automaticky; správu explicitních oprávnění provádí subjekty oprávnění na mikrofrontendu NPEZ nebo správce přes administrátorské GUI.

2.1.3.1 Implicitní oprávnění

Jedná se o oprávnění vyplývající ze zákona nebo z rozhodnutí orgánu veřejné moci. Jsou načítána z REZA a v rámci Registru oprávnění není umožněno jejich editování.

2.1.3.2 Explicitní oprávnění

Jedná se o oprávnění, která opravňující subjekty udělují explicitně, z vlastního rozhodnutí. Uživatelé mohou vytvářet nová, případně editovat existující oprávnění.

2.1.4 Zaslání notifikací o udělení oprávnění

Při změně (vzniku, zániku, postoupení) explicitního oprávnění je prostřednictvím Notifikačního systému zaslána zpráva opravňujícímu i oprávněnému uživateli.

2.1.5 Autorizace k oprávnění

Registr oprávnění poskytuje informace o oprávnění systému JSU. K oprávnění jsou uživatelé, přihlášení do dalších systémů, autorizováni prostřednictvím systému JSU v Access Tokenu a v UserInfo.

2.2 Vnitřní logika (např. zpracování dat, ukládání, validace)

2.3 Vazby na jiné komponenty

2.3.1 Zdrojové systémy

2.3.1.1 REZA

Ze systému REZA se načítají a aktualizují implicitní oprávnění.

2.3.1.2 KZR (KRP, KRZP, KRPZS)

Z KZR se načítají identifikátory pacientů (RID + AIFO), identifikátory zdravotnických pracovníků (KRZP_ID + AIFO) a identifikátory poskytovatelů zdravotních služeb (IČO).

2.3.1.3 NPEZ a EZkarta

Mikrofronendy na systémech NPEZ a EZkarta poskytují rozhraní pro administraci explicitních oprávnění uživatelů.

2.3.2 Cílové systémy

2.3.2.1 JSU

Při autentizaci uživatele JSU načte oprávnění, která má uživatel udělená, a autorizuje jej dalším systémům pro přístup k těmto oprávněním.

2.3.2.2 Systém notifikací

Při změně oprávnění je oprávněnému i opravňujícímu zaslána notifikace o oprávnění.

2.3.2.3 Auditní a logovací systém

Při změně oprávnění je do auditního a logovacího systému zaslán záznam o provedené změně.

3 Vnější rozhraní (API)

3.1 Popis poskytovaných služeb (např. REST API, SOAP, jiná)

Mikrofrontend pro administraci oprávnění na portálu NPEZ.

REST API pro předání oprávnění přihlašovaných uživatelů systému JSU.

3.2 Formát výměny dat (např. JSON, XML)

Registr oprávnění používá k výměně dat formát **JSON**.

3.3 Autentizace/autorizace (např. eIDAS, OAuth2, JWT, NIA...)

Autentizace a autorizace systémem JSU. V rámci JSU je možné využít:

- NIA pro autentizaci občanů
- NIA a EZCA pro autentizaci zdravotních pracovníků a zástupců PZS.
- CAAIS pro autentizaci OVM.

Autentizace JSU využívá OIDC.

3.4 Popis koncových bodů (endpointů) včetně:

Metoda	Endpoint	Popis
GET	/sablon/seznam	Načtení seznamu šablon oprávněníf.
GET	/opraveni/prijata	Metoda pro načtení seznamu opravňujících osob.
GET	/opraveni/udeleno	Načtení seznamu oprávnění udělených daným pacientem.
POST	/opraveni/vytvor	Vytvoření oprávnění přes GUI.
PUT	/opraveni/uprav	Editace oprávnění přes GUI.
GET	/opraveni/over	Metoda pro ověření rozsahu a obsahu oprávnění.
POST	/subjekt/vytvor	Metoda slouží k zápisu nového subjektu, který vznikl v KZR.

3.5 URL

Base URL služeb podle katalogu ...TODO

3.6 Parametry

3.6.1 GET /sablon/seznam

položka	datový typ	popis
Autentizace a autorizace bearer access tokenem	JWTToken	Access Token pro autorizaci požadavku. Access token (ve formátu JWT) se předává jako Bearer token v hlavičce zprávy.
ZadostID	GUID	ID zasílané žádosti
Datum	DateTime	Datum zaslání žádosti

3.6.2 GET /opraveni/prijata

položka	datový typ	popis
OpravenaOsoba.Typ	int	Typ identifikátoru oprávněné osoby – enumeration: <ul style="list-style-type: none"> • RID = 10 • KRZPID = 20 • ICO = 30
OpravenaOsoba.Hodnota	long	Identifikátor osoby
ZadostID	GUID	ID zasílané žádosti
Datum	DateTime	Datum zaslání žádosti

3.6.3 GET /opraveni/udelena

položka	datový typ	popis
Autentizace a autorizace bearer access tokenem	JWTToken	Access Token pro autorizaci požadavku. Access token (ve formátu JWT) se předává jako Bearer token v hlavičce zprávy.
ZadostID	GUID	ID zasílané žádosti
Datum	DateTime	Datum zaslání žádosti

3.6.4 POST /opraveni/vytvor

položka	datový typ	popis
Autentizace a autorizace bearer access tokenem	JWTToken	Access Token pro autorizaci požadavku. Access token (ve formátu JWT) se předává jako Bearer token v hlavičce zprávy.
NoveOpraveni	Opraveni	JSON struktura nového oprávnění
ZadostID	GUID	ID zasílané žádosti

Datum	DateTime	Datum zaslání žádosti
-------	----------	-----------------------

3.6.5 PUT /opraveni/uprav

položka	datový typ	popis
Autentizace a autorizace bearer access tokenem	JWTToken	Access Token pro autorizaci požadavku. Access token (ve formátu JWT) se předává jako Bearer token v hlavičce zprávy.
NoveOpraveni	Opraveni	JSON struktura nového oprávnění
ZadostID	GUID	ID zasílané žádosti
Datum	DateTime	Datum zaslání žádosti

3.6.6 GET /opraveni/over

položka	datový typ	popis
Zadatel	string	ID osoby.
VolajícíSluzba	string	ID služby, žádající o ověření
TypZdravotníhoZaznamu	Int [0..1]	Typ záznamu, ke kterému se oprávnění ověřuje.
OpravnujícíOsoba	IdentifikaceOsoby	Identifikace osoby, která oprávnění udělila.
OpravenaOsoba	IdentifikaceOsoby	Identifikace osoby, která oprávnění obdržela.
ZadostID	GUID	ID zasílané žádosti
Datum	DateTime	Datum zaslání žádosti

3.6.7 POST /subjekt/vytvor

položka	datový typ	popis
Subjekt	IdentifikaceSubjektu	ID vytvářeného subjektu.
ZadostID	GUID	ID zasílané žádosti
Datum	DateTime	Datum zaslání žádosti

3.7 Struktura odpovědi

3.7.1 GET /sablonaseznam

položka	datový typ	popis
Sablony	SablonaOpraveni [0..*]	Pole šablon, podle kterých může uživatel vytvořit oprávnění.

ZadostID	GUID	ID Žádosti, na kterou se odpověď posílá.
OdpovedID	GUID	ID odpovědi.
Datum	DateTime	Datum odpovědi.
Stav	string	Stav chyba/v pořádku.
ChybyZpracovani	string	Popis chyby.

3.7.2 GET /opraveni/prijata

položka	datový typ	popis
Osoba	IdentifikaceOsoby [0..*]	Pole id osob, ke kterým má uživatel udělená oprávnění.
ZadostID	GUID	ID Žádosti, na kterou se odpověď posílá.
OdpovedID	GUID	ID odpovědi.
Datum	DateTime	Datum odpovědi.
Stav	string	Stav chyba/v pořádku.
ChybyZpracovani	string	Popis chyby.

3.7.3 GET /opraveni/udelena

položka	datový typ	popis
Opraveni	Opraveni [0..*]	Pole oprávnění, která uživatel udělil
ZadostID	GUID	ID Žádosti, na kterou se odpověď posílá.
OdpovedID	GUID	ID odpovědi.
Datum	DateTime	Datum odpovědi.
Stav	string	Stav chyba/v pořádku.
ChybyZpracovani	string	Popis chyby.

3.7.4 POST /opraveni/vytvor

položka	datový typ	popis
ZadostID	GUID	ID Žádosti, na kterou se odpověď posílá.
OdpovedID	GUID	ID odpovědi.
Datum	DateTime	Datum odpovědi.
Stav	string	Stav chyba/v pořádku.
ChybyZpracovani	string	Popis chyby.

3.7.5 PUT /opraveni/uprav

položka	datový typ	popis
ZadostID	GUID	ID Žádosti, na kterou se odpověď posílá.
OdpovedID	GUID	ID odpovědi.
Datum	DateTime	Datum odpovědi.
Stav	string	Stav chyba/v pořádku.
ChybyZpracovani	string	Popis chyby.

3.7.6 GET /opraveni/over

položka	datový typ	popis
Stav	string	Ověření oprávnění.
ZadostID	GUID	ID Žádosti, na kterou se odpověď posílá.
OdpovedID	GUID	ID odpovědi.
Datum	DateTime	Datum odpovědi.
Stav	string	Stav chyba/v pořádku.
ChybyZpracovani	string	Popis chyby.

3.7.7 POST /subjekt/vytvor

položka	datový typ	popis
ZadostID	GUID	ID Žádosti, na kterou se odpověď posílá.
OdpovedID	GUID	ID odpovědi.
Datum	DateTime	Datum odpovědi.
Stav	string	Stav chyba/v pořádku.
ChybyZpracovani	string	Popis chyby.

3.8 HTTP kódy a chybové stavy

http 200 – úspěšné provedení

http 401 – chyba autentizace

http 404 – chybná URL, nenalezeno

http 500 – neočekávaná chyba

4 Testovací scénáře (volitelné)

4.1 Přehled testovacích scénářů

4.2 Apod.

5 Bezpečnostní opatření

5.1 Způsob zabezpečení komunikace

5.2 Autentizace

5.3 Šifrování, auditní logy, role

5.4 Apod.

6 Provozní požadavky (volitelné)

6.1 Nároky na infrastrukturu

6.2 Možnosti škálování