

ELEKTRONIZACE ZDRAVOTNICTVÍ

KMENOVÝ REGISTR

ZDRAVOTNÍCKÝCH PRACOVNÍKŮ

Účel, funkce a vnější API rozhraní



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

Obsah

1	Účel Kmenového registru zdravotnických pracovníků:.....	5
1.1	Funkční přínos KRZP v rámci systému.....	5
1.2	Zákonné požadavky, které KRZP naplňuje	5
1.3	Cílové skupiny uživatelů	5
2	Funkce komponenty:.....	8
2.1	Přehled hlavních funkcí	8
2.2	Vnitřní logika (např. zpracování dat, ukládání, validace).....	8
2.3	Vazby na jiné komponenty	8
3	Vnější rozhraní (API)	9
3.1	Popis poskytovaných služeb	9
3.2	Formát výměny dat.....	10
3.3	Autentizace/autorizace	10
3.4	Popis koncových bodů (endpointů)	10
3.5	URL.....	11
3.6	Metody	11
3.7	Parametry	12
3.8	Struktura odpovědi	13
3.9	HTTP kódy a chybové stavy	13
4	Bezpečnostní opatření	14
4.1	Požadavky na zabezpečení datových rozhraní	14
4.2	Autentizace	14
4.3	Šifrování, auditní logy, role.....	14

Seznam zkratk a pojmů

Zkratka	Význam
AIFO	Agendový identifikátor fyzické osoby
AIS	Agendový informační systém
AISC	Agendový informační systém cizinců
AISEO	Agendový informační systém evidence obyvatel
BSI	Bezvýznamový směrový identifikátor

CIS	AIS Cizinci; Cizinecký informační systém
ČLK	Česká lékařská komora
ČP	Číslo pojištěnce
DRID	Dočasný RID
EZ	Elektronické zdravotnictví, eHealth
EZCA	Certifikační autorita elektronického zdravotnictví (MZČR)
GUI	Grafické uživatelské rozhraní (graphical user interface)
IČO	Identifikační číslo například poskytovatele zdravotních služeb
ID ZP	Identifikátor zdravotnického pracovníka
IDR	Integrované datové rozhraní (zdravotnictví) Alternativní zkratka pro preferovanou zkratku IDRR
IDRR	Integrované datové rozhraní resortu (Dle zákona Integrované datové rozhraní zdravotnictví, zkráceně Integrované datové rozhraní)
JSU	Jednotná správa uživatelů
KIS	Klinický informační systém
Kmenový údaj	Informace, kterou využívá oprávněná osoba, aniž by ověřovala její správnost
KRP	Kmenový registr pacientů
KRPZS	Kmenový registr poskytovatelů zdravotních služeb
KRZP	Kmenový registr zdravotnických pracovníků
NIA	Národní identita ČR
NIS	Nemocniční informační systém
NPEZ	Národní portál elektronického zdravotnictví
NRPZS	Národní registr poskytovatelů zdravotních služeb
NRZP	Národní registr zdravotnických pracovníků
PZS	Poskytovatel zdravotních služeb
REST API	REpresentational State Transfer API
REZA	Registr zastupování
RID	Bezvýznamový identifikátor pacienta (resortní ID)
ROB	Registr obyvatel
ROS	Registr osob
RÚIAN	Registr územní identifikace, adres a nemovitostí
SÚKL	Státní ústav pro kontrolu léčiv
SZÚ	Státní zdravotní ústav
ZP - zdravotní pojišťovna	Zdravotní pojišťovna

ZP - zdravotnický pracovník	Zdravotnický pracovník
ZR	Základní registry

1 Účel Kmenového registru zdravotnických pracovníků:

Kmenový registr zdravotnických pracovníků (KRZP) je autoritativním zdrojem dat.

Registr je napojen na Národní registr zdravotnických pracovníků (NRZP), prostřednictvím kterého se provádí zápis všech údajů a jejich průběžná aktualizace. NRZP je napojen na Informační systém základních registrů, ze kterých čerpá aktuální referenční údaje.

1.1 Funkční přínos KRZP v rámci systému

Kmenový registr zdravotnických pracovníků

- vede jednoznačné, aktuální a platné údaje o zdravotnických pracovnících,
- slouží k identifikaci pracovníků a jako zdroj údajů pro poskytovatele zdravotních služeb a dalších oprávněných osob podle zákona,
- obsahuje zaručené údaje o dosaženém vzdělání a odbornosti pracovníků, které budou v budoucnu sloužit jako alternativa prokazování diplomem či certifikátem.

1.2 Zákonné požadavky, které KRZP naplňuje

Kmenový registr zdravotnických pracovníků je zřízen zákonem č. 325/2021 Sb., o elektronizaci zdravotnictví, kde

- v § 21, odst. 1), je specifikován rozsah vedených údajů,
- v § 21, odst. 2) a 3), jsou specifikovány Zapisující osoby, tj. editoři, a způsob vedení zápisu,
- v § 22 specifikuje Oprávněné osoby, tj. čtenáře údajů,
- v § 25 stanovuje vazbu na základní registry a agendové informační systémy a popisuje jejich režimy.

1.3 Cílové skupiny uživatelů

Kmenový registr zdravotnických pracovníků má nastavena oprávnění pro jednotlivé role v systému dle Zákona č. 325/2021 Sb. o elektronizaci zdravotnictví. Oprávněné a zapisující osoby mají přístup k potřebným informacím a službám, zatímco neoprávněné osoby jsou omezeny v přístupu.

1.3.1 Zapisující osoba

Dále též jako Editor, je právnická, fyzická nebo podnikající fyzická osoba, organizační složka státu nebo organizační složka územního samosprávného celku zapisující údaje do KRZP, v rozsahu dle Zákona č. 325/2021 Sb.

Editory kmenových údajů jsou:

Primární editor	Primární editor je zodpovědný za založení a samotnou existenci celého záznamu.
Sekundární editor	Sekundární editor edituje existující záznam.
Lékařské komory	<ul style="list-style-type: none">• Česká lékařská komora• Česká stomatologická komora

	<ul style="list-style-type: none"> Česká lékárnická komora
MZD	Ministerstvo zdravotnictví ČR.
Poskytovatel zdravotních služeb (PZS)	<p>Fyzická nebo právnická osoba, která má oprávnění k poskytování zdravotních služeb podle zákona č. 372/2011 Sb., o zdravotních službách.</p> <p>Poskytovatelé zdravotních služeb jsou lékaři, nelékařští zdravotničtí pracovníci, nemocnice a další zdravotnická zařízení, kteří ke své činnosti mají oprávnění krajského úřadu anebo ministerstva.</p> <p>Subjekt je evidovaný v KRPZS.</p>
Pověřená organizace	Pověřené organizace jsou Institut postgraduálního vzdělávání ve zdravotnictví a Národní centrum ošetřovatelství a nelékařských zdravotnických oborů
Soud	Soudy ČR
ÚZIS ČR	Ústav zdravotnických informací a statistiky ČR
Vzdělávací zařízení	Vzdělávací zařízení jsou např. fakulty, střední školy a vyšší odborné školy, a akreditovaná zařízení
Zdravotnický Pracovník	<p>Lékaři a nelékařští zdravotničtí pracovníci.</p> <p>Osoba je evidovaná v KRZP.</p>

1.3.2 Oprávněná osoba

Dále též jako Čtenář, je právnická, fyzická nebo podnikající fyzická osoba, organizační složka státu nebo organizační složka územního samosprávného celku, která je oprávněna využívat služby Integrovaného datové rozhraní v rozsahu dle Zákona č. 325/2021 Sb.

Čtenáři kmenových údajů jsou:

ČSSZ	Česká správa sociálního zabezpečení
Institut PZS	Institut posuzování zdravotního stavu
Lékařské komory	<ul style="list-style-type: none"> Česká lékařská komora Česká stomatologická komora Česká lékárnická komora
Krajský úřad	Krajský úřad
MO ČR	Ministerstvo obrany ČR
MS ČR	Ministerstvo spravedlnosti ČR
MV ČR	Ministerstvo vnitra ČR
MZD	Ministerstvo zdravotnictví ČR
Osoba usazená	Uchazeč, který vykonává na území České republiky soustavně zdravotnické povolání nebo povolání jiného odborného pracovníka
Poskytovatel zdravotních služeb (PZS)	<p>Fyzická nebo právnická osoba, která má oprávnění k poskytování zdravotních služeb podle zákona č. 372/2011 Sb., o zdravotních službách.</p> <p>Poskytovatelé zdravotních služeb jsou lékaři, nelékařští zdravotničtí pracovníci, nemocnice a další zdravotnická zařízení, kteří ke své činnosti mají oprávnění krajského úřadu anebo ministerstva.</p> <p>Subjekt je evidovaný v KRPZS</p>
Pověřená organizace	Pověřené organizace jsou Institut postgraduálního vzdělávání ve zdravotnictví a Národní centrum ošetřovatelství a nelékařských zdravotnických oborů

Provozovatel NCP (Národní kontaktní místo)	Provozovatel Národního kontaktního místa pro elektronické zdravotnictví (NCPeH – National Contact Point for eHealth).
SÚKL	Státní ústav pro kontrolu léčiv
ÚZIS ČR	Ústav zdravotnických informací a statistiky ČR
Zdravotní pojišťovna	Zdravotní pojišťovna je specializovaná zdravotní a finanční instituce, jejímž hlavním úkolem je provádět všeobecné zdravotní pojištění.
Zdravotnický pracovník	Lékaři a nelékařští zdravotničtí pracovníci. Osoba je evidovaná v KRZP.

2 Funkce komponenty:

2.1 Přehled hlavních funkcí

V KRZP jsou implementovány funkce, které zajišťují všechny potřebné operace se záznamy o pracovnících, a průběžnou synchronizaci kmenových údajů s Národním registrem zdravotnických pracovníků, který je primárním systémem pro editaci údajů.

2.2 Vnitřní logika zpracování dat a validací

Kmenová data jsou na vstupu do systému průběžně validována, a to z různých hledisek

2.2.1 Formátová validace

Ověřuje se, že data na vstupu splňují předdefinovaná formátovací pravidla, zejména se jedná o tyto

- validace datumů – délky číselných hodnot (např. pro dny, měsíce, roky), a také to, zda je datum platné v kalendáři
- validace telefonních čísel – zda splňuje délku a pořadí znaků
- validace adres elektronické pošty

2.2.2 Obsahová validace

Jedná se zejména o faktickou správnost vstupních údajů:

- validace adres proti RÚIAN
- validace IČO proti Registru osob
- validace proti Centrálním číselníkům EZ

2.3 Vazby na jiné komponenty

Kmenový registr zdravotnických pracovníků kooperuje s těmito systémy:

2.3.1 Centrální služby

- Registr oprávnění
- Správa číselníků
- Systém notifikací
- JSÚ a SSR
- Žurnál činností

2.3.2 Veřejná rozhraní

- NPEZ
- EZKarta
- API rozhraní

3 Vnější rozhraní (API)

3.1 Popis poskytovaných služeb

3.1.1 Režim volání služeb KRZP a principy synchronizace dat

REST API služeb KRZP umožňuje efektivní volání ze strany klientů.

Každý požadavek na REST API KRZP obsahuje standardizovanou sadu dat, která umožňuje jednoznačnou identifikaci, trasování a auditování dotazu.

- Identifikace žádosti – z pohledu žadatele. Umožňuje identifikovat dotaz i odpověď pro potřeby auditního sledování ze strany klienta
- Důvod žádosti – textový popis důvodu / účelu volání rozhraní kmenových registrů
- Datum žádosti – datum vzniku žádosti z pohledu žadatele

3.1.2 Komunikační schéma pro využívání služeb KRZP

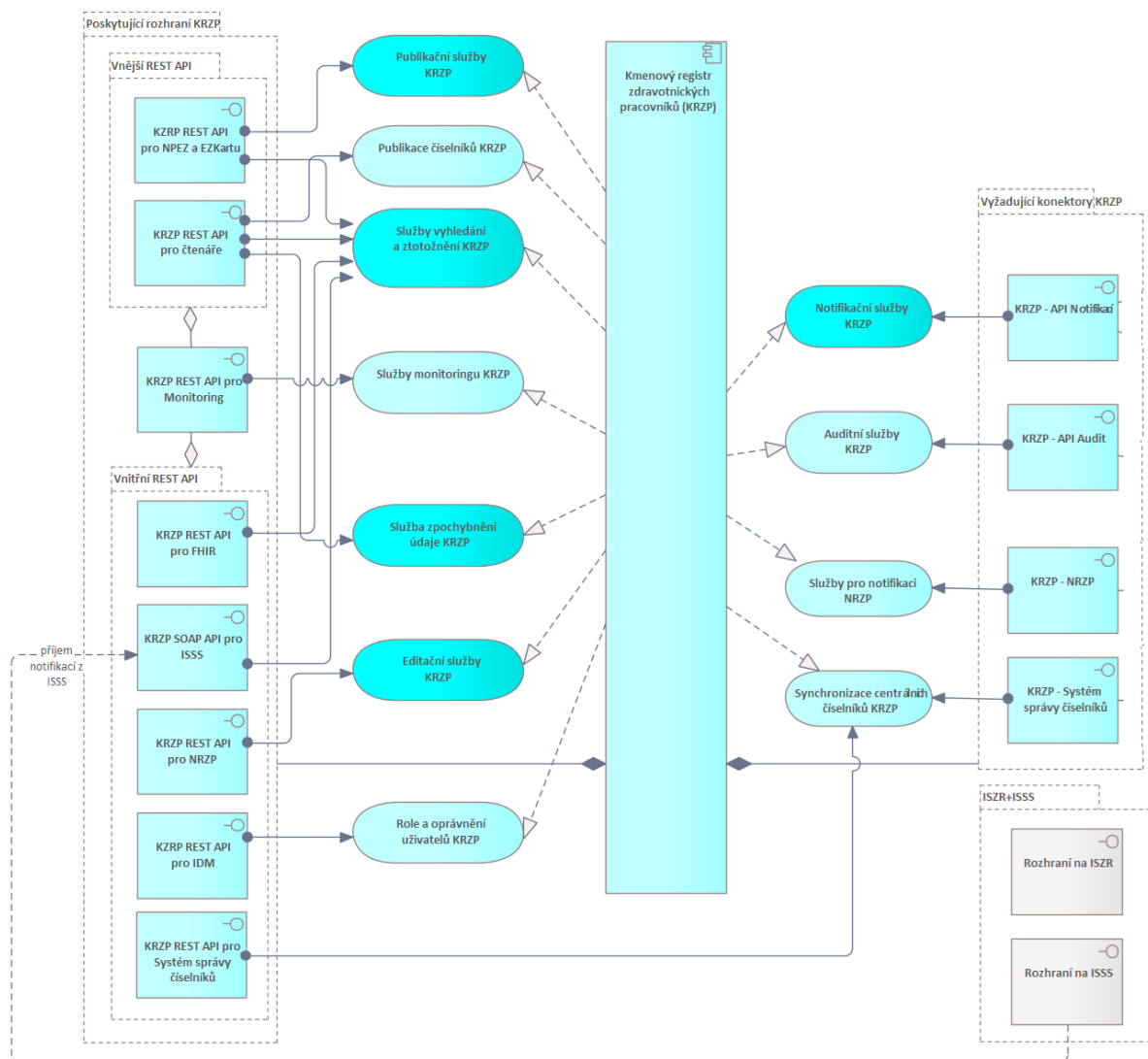


Diagram architektonického hlediska spolupráce KRZP – se zaměřením na rozhraní a napojení na okolní systémy a zdroje dat.

3.2 Formát výměny dat

Datové formáty používané v rámci KZR jsou:

- **JSON** (JavaScript Object Notation)
- pro hromadné zpracování dat jsou přílohy ve formátu **XML**,
- pro komunikaci se subjekty přístupujícími přes rozhraní ISSS jsou k dispozici **SOAP** rozhraní.

3.3 Autentizace/autorizace

Autentizace k REST API službám KRZP probíhá pomocí systémových certifikátů vydaných některou z definovaných CA. Vydávání a správa vydávaných autentizačních certifikátů je řešena v centrálních službách EZ.

3.4 Popis koncových bodů (endpointů)

KRZP umožňuje napojení externích uživatelů a systémů pomocí těchto rozhraní:

3.4.1 REST API pro čtenáře KRZP

Rozhraní je určeno pro všechny subjekty s rolí Oprávněná osoba – čtenář.

K dispozici jsou tyto metody

Název metody	Popis metody	Dotaz (parametry)	Odpověď
GET VyhledejPodleKRZPID	Metoda pro vyhledání pracovníka podle KRZP ID	Tbd	Tbd
GET VyhledejPodleJmenoPr ijmeniDatumNarozeni	Metoda pro vyhledání pracovníka dle jména, příjmení a data narození.	Tbd	Tbd
GET VyhledejPodleZamestn avatele	Metoda pro vyhledání seznamu pracovníků podle IČO zaměstnavatele	Tbd	Tbd
GET VyhledejPodleUlozky		Tbd	Tbd

Detailní popis metod je uveden v kapitole 3.6 Metody.

3.4.2 REST API Číselníky

Rozhraní je určeno pro všechny subjekty s rolí Oprávněná osoba – čtenář.

K dispozici jsou následující metody:

Název metody	Popis metody	Dotaz (parametry)	Odpověď
GET CiselnikStat	Metoda pro publikaci číselníku států.	zadost: ZadostOVyhledaniC iselniku	OdpovedVyhledaniCise lniku
GET CiselnikDruhDok ladu	Metoda pro publikaci číselníku druhů dokladů.	zadost: ZadostOVyhledaniC iselniku	OdpovedVyhledaniCise lniku

Název metody	Popis metody	Dotaz (parametry)	Odpověď
GET CiselnikZdravotniPojistovna	Metoda pro publikaci číselníku zdravotních pojišťoven.	zadost: ZadostOVyhledaniCiselniku	OdpovedVyhledaniCiselniku
GET CiselnikPohlavi	Metoda pro publikaci číselníku pohlaví.	zadost: ZadostOVyhledaniCiselniku	OdpovedVyhledaniCiselniku

3.5 URL

Služby jsou publikované v rozhraní <https://apidoc.krzp.xxx.cz/index.html> (nyní nefunkční - bude doplněno až po finálním nasazení na produkční prostředí).

3.6 Metody

Kmenový registr poskytuje následující služby:

3.6.1 Vyhledání kmenových údajů pracovníka

Životní situace: Potřeba vyhledání kmenových údajů pracovníka

Určeno pro subjekty: Oprávněné osoby – čtenáři kmenových údajů

API: REST API pro čtenáře údajů

Seznam dostupných GET metod pro vyhledání údajů pacienta:

API metody	Popis
GET	Metoda vyhledá pracovníka

3.6.2 Reklamace kmenového údaje pracovníka

Životní situace: Uživatel má pochybnost o správnosti kmenového údaje.

Určeno pro subjekty: Oprávněné osoby – čtenáři kmenových údajů

API: REST API pro čtenáře údajů

API metoda: (POST) ReklamujUdaj

Vstupní data:

Název	Typ	Multiplicita	Popis
KRZPID	Long	[0...1]	
UlozkaId	String	[0...1]	Úložka ORG
UlozkaRef	Int	[0...1]	Úložka ORG - reference na záznam v úložce
DatumReklamace	DateTime	[1]	
Reklamujici	Reklamujici	[1]	Identifikace reklamující osoby. Dle legislativy reklamaci může založit jakýkoli čtenář registru
PolozkyReklamace	UdajReklamace	[1...*]	

Zduvodneni	String	[0...1]	Důvod reklamace
PopisReklamace	String	[1]	

Popis: Metoda pro reklamaci kmenového údaje iniciovaná čtenářem.

3.6.3 Administrace notificačních služeb

Životní situace: Potřeba administrace notifikací o změně kmenových údajů

Určeno pro subjekty: Oprávněné osoby – čtenáři kmenových údajů

API: REST API pro čtenáře údajů

Seznam dostupných metod pro administraci notifikací:

API metody	Popis
POST ZalozOdberNotifikaci	Metoda pro založení odběru (subscribe) notifikace pro definovanou sadu pracovníků a definovaný kanál notifikace. kriteria: systém(registr)?typ=identifikátor příklad KRZP?ico=1234567891
PUT ZrusOdberNotifikaci	Zrušení záznamu odběru notifikace podle ID
GET VyhledejOdberNotifikaciPZS	Metoda pro zjištění aktuálně platných odběrů notifikací o zdravotnických pracovnících, které má uživatel registrovány. Vyhledání aktivních registrací k odběru notifikací. (subscribe) podle ID - vrátí registraci nebo 404 podle kriteria (id je null) - vrátí podle kriteria, např. "KRZP" všechny odběry pracovníků pro IČO id je null, kriteria je null - vrátí všechny registrace pro žádající IČO (PZS) Vrací kolekci objektů

3.7 Parametry

Rozhraní na vstupu očekává jednotnou strukturu dotazů pro každou metodu **ZadostO...**

Název	Typ	Multiplicita	Popis
ZadostInfo	KZRDotaz	[1]	Univerzální datový objekt
ZadostData	DATA	[1]	Návratový datový objekt podle typu metody

Každá žádost podaná do KRZP musí být opatřena atributem **KZRDotaz**, který obsahuje:

- Identifikátor žádosti, který poskytne dotazující strana.
- Důvodem / účelem podání žádosti. V případě dotazování do navazujících systémů je použitý tento důvod.

Název	Typ	Multiplicita	Popis
ZadostId	GUID	[1]	Korelační identifikátor žádosti

Ucel	string	[1]	Důvod / účel podání žádosti. V případě dotazování do navazujících systémů je použitý tento důvod.
Datum	DateTime	[1]	

3.8 Struktura odpovědi

Rozhraní poskytuje jednotný formát odpovědi v následující struktuře:

Název	Typ	Multiplicita	Popis
OdpovedInfo	KZROdpoved	[1]	Univerzální datový objekt
OdpovedData	DATA	[1]	Návratový datový objekt podle typu metody

Struktura datového typu **KZROdpoved**

Název	Typ	Multiplicita	Popis
ZadostId	GUID	[1]	ID dotazu, který byl přijat
OdpovedId	GUID	[1]	ID odpovědi
Stav	String	[1]	Stav zpracování dotazu, použity jsou hodnoty: OK, Varovani, Chyba.
SubStav	String	[0...1]	Doplňující informace k atributu „Stav“,
Popis	String	[0...1]	
ChybyZpracovani	String	[0...1]	Kolekce chyb, nebo varování, které vznikly při zpracování požadavku

3.9 HTTP kódy a chybové stavy

Rozhraní vrací v odpovědi standardní chybové kódy:

Status	Výsledek	Zpráva
200	OK	úspěch
201	Created	něco bylo vytvořeno
400	Bad Request	špatný požadavek
401	Unauthorized	chybí přihlášení
404	Not Found	nenalezeno
500	Internal Server Error	chyba na straně serveru

4 Bezpečnostní opatření

4.1 Požadavky na zabezpečení datových rozhraní

Všechna připojení k externím systémům zahrnujícím výměnu dat / citlivé funkce jsou autentizována;

Všechna připojení k externím systémům s funkcí výměny dat / citlivých funkcí budou používat účet s nastavenými minimálními potřebnými oprávněními;

Všechny autentizační údaje k externím systémům a aplikacím budou uloženy šifrovaně v úložišti s omezeným přístupem (nikoliv ve zdrojovém kódu);

4.1.1 Bezpečnost datových rozhraní

Jsou použity bezpečné autentizační mechanismy, pro ověřování a autorizaci přístupu k API. Je nastaven Rate Limiting a Throttling pro omezování počtu požadavků na API za určité časové období, aby se zabránilo útokům typu DoS (Denial of Service).

Jsou použity API brány pro centralizovanou správu zabezpečení API, autentizaci, autorizaci, a monitorování přístupu.

4.2 Autentizace

K datovým API službám pro strojové čtení dat se Poskytovatelé zdravotních služeb autentizují výhradně pomocí systémových certifikátů vydaných EZCA.

Informační systémy se budou přihlašovat s využitím asymetrické kryptografie a klientského certifikátu v rámci TLS protokolu.

U klientského certifikátu bude ověřována jeho platnost (minimálně vydávající certifikační autorita, účely a platnost) a použité klíče.

Přihlašování bude probíhat přes bezpečné (šifrované) protokoly.

4.3 Šifrování, auditní logy, role

4.3.1 Bezpečnost komunikačních sítí

SSL/TLS šifrování je použito pro všechna připojení, která:

- vyžadují autentizaci uživatele;
- souvisejí s procesem změny hesla;
- odesílají nebo přijímají data/citlivé funkce;
- souvisí se správou aplikace;

Přenos citlivých dat a/nebo osobních údajů je vždy šifrován.

4.3.2 Auditní logování

Všechny operace prováděné uživateli nebo automaticky systémem registrů jsou logovány a ukládány do Žurnálu činností, ve smyslu § 37, zákona č. 325/2021 Sb o elektronizaci zdravotnictví.

Auditní záznamy obsahují minimálně následující informace (relevantní z nich):

- systém, zařízení nebo aplikaci, který záznam vygenerovaly;
- identifikátor (uživatelské jméno, ID procesu, IP adresu, terminál apod.) osoby, programu, služby či zařízení, které je zdrojem zaznamenané události;
- datum a čas události;
- popis důvodu události (přístup uživatele, systémová chyba apod.);
- v případě záznamu o přístupu ještě:
 - zdroj, ke kterému bylo přistoupeno (informace, aplikace, disk, síť apod.);
 - typ přístupu (čtení, modifikace, zobrazení ve výpisy, SQL dotaz, smazání apod.);
 - informaci o tom, kde jde o autorizovaný/anonymní/neautorizovaný přístup (resp. pokus o přístup);
 - uživatelské oprávnění;
 - terminál, nebo systém, ze kterého byl přístup (či pokus o přístup) učiněn.

Tyto záznamy:

- jsou ukládány po dobu 18 měsíců – v centrálním úložišti,
- lokálně budou chráněny před neoprávněným přístupem, a
- bude možné odesílat do centrálního LogManager / SIEM (protokolem syslog).

4.3.3 Uživatelské role

Detailní popis uživatelských rolí je uveden v kapitole 1.3 Cílové skupiny uživatelů.

V principu jsou v Kmenovém registru nastaveny tyto role:

4.3.3.1 Editor

je právnická, fyzická nebo podnikající fyzická osoba, organizační složka státu nebo organizační složka územního samosprávného celku **zapisující údaje do kmenových zdravotnických registrů**, v rozsahu dle Zákona č. 325/2021 Sb.

4.3.3.2 Čtenář

je právnická, fyzická nebo podnikající fyzická osoba, organizační složka státu nebo organizační složka územního samosprávného celku, která **je oprávněna využívat kmenové zdravotnické registry** v rozsahu dle Zákona č. 325/2021 Sb.

4.3.3.3 Věcný správce

je fyzická osoba, která zajišťuje výkon činností věcné správy dat nad svěřenými daty a dbá na jejich kvalitu a správnost. Prakticky vykonává některé operace s kmenovými údaji, jako např. Slučování pacientů, Rozdělení pacientů, Rollback sloučení, Mazání záznamů apod.

4.3.3.4 Administrátor

je fyzická osoba zodpovědná za provoz a správu systému.