Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Projekt „**Strategické řízení rozvoje elektronického zdravotnictví v resortu MZ**“,
registrační číslo CZ.03.4.74/0.0/0.0/15_025/0006212,
je spolufinancován Evropskou unií.

ZPRACOVÁNÍ METODIK TVORBY NÁSTROJŮ PRO IMPLEMENTACI NÁRODNÍ STRATEGIE ELEKTRONICKÉHO ZDRAVOTNICTVÍ

Aktualizace zpracovaných TO-BE modelů EA prioritních opatření, řešení dle akčního plánu elektronizace

eID - Elektronická Identita

Projekt:	Strategické řízení rozvoje elektronického zdravotnictví v resortu MZ, registrační číslo CZ.03.4.74/0.0/0.0/15_025/0006212 je spolufinancován Evropskou unií		
Klíčová aktivita:	Zpracování metodik tvorby nástrojů pro implementaci národní strategie elektronického zdravotnictví		
Datum:	12. 4. 2019	Stav:	Finální verze
Část díla:	Aktualizace zpracovaných TO-BE modelů EA prioritních opatření, řešení dle akčního plánu elektronizace		
Název produktu:	eID – Elektronická Identita		
Autor:	Asseco Central Europe, a.s.		
Zhotovitel:	Asseco Central Europe, a.s.		
Objednatel:	Ministerstvo zdravotnictví ČR		
Verze:	1.0		

Schválení

Jméno	Podpis	Pozice	Datum
Ing. Martin Zeman		Sponzor projektu	12.4.2019
Ing. Jiří Borej		Hlavní uživatel	12.4.2019

Distribuční seznam

Jméno	Subjekt / organizační jednotka	Datum	Verze
Ing. Martin Zeman	Ministerstvo zdravotnictví ČR	12.4.2019	1.0
Ing. Jiří Borej	Ministerstvo zdravotnictví ČR	12.4.2019	1.0

Přehled provedených změn

Číslo verze	Kapitola / strana	Předmět aktualizace	Účinnost (datum)
1.01		Překlopení výstupu do formalizované šablony dokumentu	4.11.2019

Dokument vznikl v rámci Klíčové aktivity 3 projektu „Strategické řízení rozvoje elektronického zdravotnictví v resortu MZ“, kde účelem projektu bylo strategické řízení a vytvoření komplexního systému metodické podpory pro realizaci aktivit elektronizace zdravotnictví. Klíčová aktivita 3 byla pak zaměřena na zpracování metodik tvorby nástrojů pro implementaci Národní strategie elektronického zdravotnictví. Dokument odráží aktuální stav poznatků ke dni schválení 12.4.2019. Architektonické modely zpracovávané pro účel elektronizace zdravotnictví se v čase mohou vyvíjet a je tedy možné, že jsou k dispozici v aktuálnější podobě v úložišti architektonických modelů. Proto bude na stránkách www.nsez.cz uveřejněn odkaz na publikační vrstvu architektonických modelů, kde budou k dispozici vždy nejnovější uvolněné verze modelů.

1. eID - Elektronická Identita

1.1 Diagram: (AA) eID - autentizace pacienta

Subsystém – eID - autentizace pacienta

Účel
Diagram zobrazuje komponenty elektronického zdravotnictví, které slouží pro autentizaci pacienta ke službám elektronického zdravotnictví.

Popis základní funkcionality subsystému
Pacient přistupuje k Národnímu zdravotnickému informačnímu portálu (NZIP), který obsahuje veřejné informace a informace a služby, konkrétnímu pacientovi (občanovi). Pro přístup k těmto službám je vyžadována autentizace a autorizace.

Autentizace pacienta je výhradně prostřednictvím služeb Národního bodu pro identifikaci (NIA). Pro různé služby eZ jsou vyžadovány různé úrovně záruk (značná, vysoká). Při využití eOP může přistoupit ke všem svým datum a službám.

NIA identifikuje pacienta, ověří záznam v ROB a identifikaci předá prostřednictvím Resortního datového rozhraní do Systému správy identit a oprávnění (IAM). V IAM proběhne ztotožnění pacienta vůči autoritativním údajům pacienta (ARP).

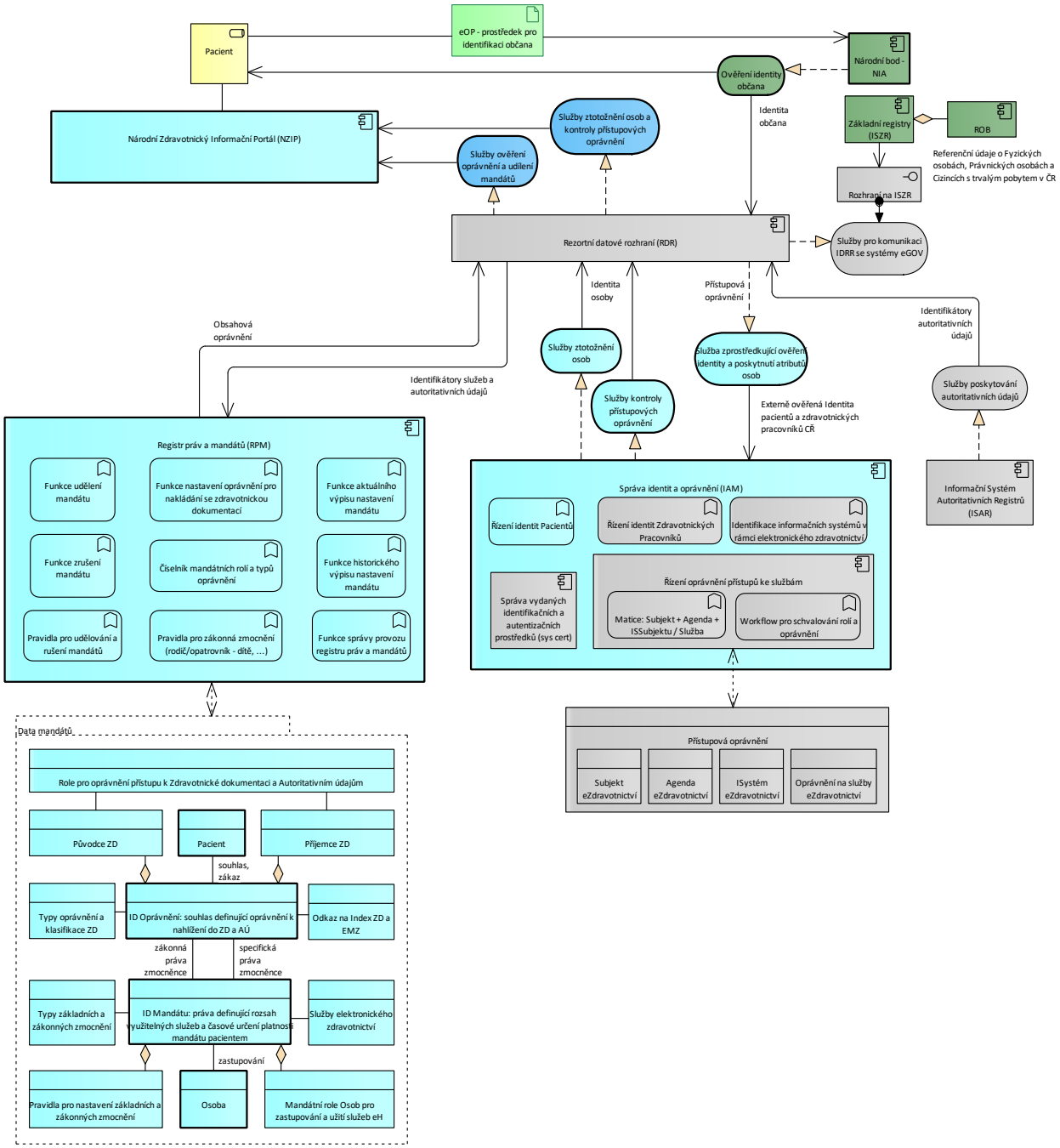
Autorizace pacienta probíhá prostřednictvím služeb Registru práv a mandátů. Pacient může pověřit pro definované úkony a služby třetí osobu. Tyto pověření může spravovat prostřednictvím služeb NZIP.

Předpoklady
Východiska
- Existence ARP - autoritativního registru pacientů

Principy a pravidla
- Autentizace pacienta pouze prostředky eGOV

Vazby
Interní
- Registr práv a mandátů - ověření mandátů pacienta
- ARP - informace o pacientovi
- IAM - ztotožnění pacienta vůči ARP

Externí
- NIA - autentizace pacienta
- ISZR, ROB - informace o pacientovi



Element Agenda eZdravotnictví

Typ	DataObject
Popis	Datový objekt, který reprezentuje část matice oprávnění - Agendu eZdravotnictví.

Element Číselník mandátních rolí a typů oprávnění

Typ	ApplicationFunction

Popis	Číselník mandátních rolí a typů oprávnění

Element Data mandátů

Typ	Grouping
Popis	Seskupení, které charakterizuje data mandátů.

Element eOP - prostředek pro identifikaci občana

Typ	Artifact
Popis	Elektronický občanský průkaz je autentizační prostředek s nejvyšší úrovní záruk dle nařízení eIDAS. Slouží pro autentizaci občana vůči elektronickým službám.

Element Funkce aktuálního výpisu nastavení mandátu

Typ	ApplicationFunction
Popis	Funkce aktuálního výpisu nastavení mandátu

Element Funkce historického výpisu nastavení mandátu

Typ	ApplicationFunction
Popis	Funkce historického výpisu nastavení mandátu

Element Funkce nastavení oprávnění pro nakládání se zdravotnickou dokumentací

Typ	ApplicationFunction
Popis	Funkce nastavení oprávnění pro nakládání se zdravotnickou dokumentací

Element Funkce správy provozu registru práv a mandátů

Typ	ApplicationFunction
Popis	Funkce správy provozu registru práv a mandátů

Element Funkce udělení mandátu

Typ	ApplicationFunction
Popis	Funkce udělení mandátu

Element Funkce zrušení mandátu

Typ	ApplicationFunction
Popis	Funkce zrušení mandátu

Element ID Mandátu: práva definující rozsah využitelných služeb a časové určení platnosti mandátu pacientem

Typ	DataObject
Popis	Mandát jako právo definující rozsah využitelných služeb eH zastupující osobou a časové určení platnosti tohoto mandátu pacientem.

Element ID Oprávnění: souhlas definující oprávnění k nahlížení do ZD a AÚ

Typ	DataObject
Popis	ID Oprávnění: souhlas definující oprávnění k nahlížení do ZD a AÚ.

Element Identifikace informačních systémů v rámci elektronického zdravotnictví

Typ	ApplicationFunction
Popis	**ÚČEL** V tomto případě se nejedná o ztotožňování osob, ale o identifikaci a ztotožnění informačních systémů. Tato identifikace a ztotožnění v praxi představuje autentizační prostředek - systémový certifikát - vydávaný Certifikační autoritou resortu jednotlivým subjektům elektronického zdravotnictví **pro účely zabezpečení komunikace** při volání Centrálních služeb EZ.

Element Informační Systém Autoritativních Registrů (ISAR)

Typ	ApplicationComponent
Popis	Informační Systém Autoritativních Registrů (ISAR) zajišťuje společné funkce pro dílčí autoritativní registry: • Autoritativní registr pacientů (ARP) • Autoritativní registr zdravotnických pacientů (ARZP) • Autoritativní registr poskytovatelů zdravotních služeb (ARPZS) a připojení těchto registrů na Rezortní Datové Rozhraní prostřednictvím služeb pro Poskytování a Editaci autoritativních údajů.

Element ISystém eZdravotnictví

Typ	DataObject
Popis	Datový objekt, který reprezentuje část matice oprávnění - Informační systém elektronického zdravotnictví.

Element Mandátní role Osob pro zastupování a užití služeb eH

Typ	DataObject
Popis	Mandátní role Osob pro zastupování a užití služeb eH

Element Matice: Subjekt + Agenda + ISSubjektu / Služba

Typ	ApplicationFunction
Popis	Funkce pro vložení, změnu a výmaz záznamu v matice oprávnění IAM, který

	je tvořen údaji: **Subjekt + Agenda + ISSubjektu** pro danou **Centrální službu elektronického zdravotnictví.** Tímto záznamem oprávnění je jednoznačně definován přístup k množině služeb pro využití konkrétním subjektem při výkonu agendy a za použití stanoveného informačního subjektu

Element Národní bod - NIA

Typ	ApplicationComponent
Popis	Národní bod pro identifikaci, někdy též Národní identitní autorita (NIA) umožňuje autentizaci občanů a ověření identity pro následné využívání elektronických služeb státu. Občan si může vybírat z různých autentizačních služeb (eOP, Jméno+heslo+SMS, v budoucnu též bankovní ID). Pro oblast zdravotnictví se bude plně využívat těchto státem garantovaných a poskytovaných služeb pro roli Pacient.

Element Národní Zdravotnický Informační Portál (NZIP)

Typ	ApplicationComponent
Popis	Portál zajišťuje vizuální rozhraní pro veřejnost, pacienty a pojištěnce, zdravotnické pracovníky, pověřené osoby, správce provozu a řízení tvorby obsahu portálu. NZIP je komponenta, která se podílí hlavní měrou na naplnění Strategického cíle 1: Zvýšení zainteresovanosti občana na péči o vlastní zdraví. Zahrnuje procesy • strategické řízení NZIP, • zdroje a financování, • řízení vztahů s partnery, • vlastní proces tvorby obsahu NZIP, • poskytování informací anonymnímu uživateli i uživatelům oprávněným (registrovaným), • zajištění technické správy a provozu.

Element Odkaz na Index ZD a EMZ

Typ	DataObject
Popis	Odkaz na Index ZD a EMZ.

Element Oprávnění na služby eZdravotnictví

Typ	DataObject
Popis	Datový objekt, který obsahuje persistentně uložený záznam oprávnění

	subjektu, agendy a informačního systému pro užití vybrané množiny služeb elektronického zdravotnictví.

Element Osoba

Typ	DataObject
Popis	Osoba

Element Ověření identity občana

Typ	ApplicationService
Popis	Služba veřejné správy zajišťující ověření identity občana nebo cizince žijícího v České republice.

Element Pacient

Typ	BusinessRole
Popis	Fyzická osoba, která přichází do kontaktu se systémem zdravotní péče v ČR v okamžiku, kdy je této roli poskytována zdravotní služba (případně speciální zdravotní služba). Role Pacient je z pohledu využívání centrálních služeb eH postavena výhradně na autentizovaném přístupu. Důvodem je poskytování citlivých osobních a zdravotnických informací na portálu NZIP v oblastech: **Dostupnost zdravotních služeb** • Elektronické objednání a časová a místní dostupnost ZP a PZS • Elektronická konzultace zdravotního stavu **Zdravotní stav a léčebná plán** • Přístup k osobním zdravotním záznamům • Mandát pro zastupování a oprávnění nahlížení do zdravotnické dokumentace • Osobní účet ve fondu plátců a úhrad **Péče o vlastní zdraví** • Zdravotní rizika pacienta • Program péče pro chronicky nemocné a z pohledu klienta služeb eZ v rámci Národního kontaktního místa je: • Rolí poskytující údaje pro přístup ke zdravotnické dokumentaci a • Žádajícím o přístup ke své zdravotnické dokumentaci **Zdravotnická dokumentace** • Index zdravotnické dokumentace • Emergency záznam pacienta

Element Pacient

Typ	DataObject
Popis	Pacient

Element Pravidla pro nastavení základních a zákonných zmocnění

Typ	DataObject
Popis	Pravidla pro nastavení základních a zákonných zmocnění

Element Pravidla pro udělování a rušení mandátů

Typ	ApplicationFunction
Popis	Pravidla pro udělování a rušení mandátů

Element Pravidla pro zákonná zmocnění (rodič/opatrovník - dítě, ...)

Typ	ApplicationFunction
Popis	Pravidla pro zákonná zmocnění (rodič/opatrovník - dítě, ...)

Element Příjemce ZD

Typ	DataObject
Popis	Příjemce ZD

Element Přístupová oprávnění

Typ	DataObject
Popis	Datové úložiště relační databáze, které zajišťuje persistentní uložení přístupových oprávnění pro užití služeb elektronického zdravotnictví pro dané subjekty a agendy vykonávané ve zdravotnictví.

Element Původce ZD

Typ	DataObject
Popis	Původce ZD

Element Registr práv a mandátů (RPM)

Typ	ApplicationComponent
Popis	Registr práv a mandátů umožňuje správu mandátů pacienta vůči dalšímu subjektu pro přístup k datům a službám eZ.

Element Rezortní datové rozhraní (RDR)

Typ	ApplicationComponent
Popis	Resortní datové rozhraní představují klíčovou komponenty IDRR, která je Integrační platformou pro subsystémy IDRR.

Element Řízení identit Pacientů

Typ	ApplicationFunction
Popis	**ÚČEL** Zajistit identifikaci a autentizaci pacienta neboli ověření a garantování identity pro přístup a využívání služeb EZ. Daný způsob nemusí být určen čistě pro elektronické služby, ale může být využit i při asistovaném způsobu využívání služeb, např. povolení k náhledu do ZD při fyzické návštěvě zdravotnického pracovníka. Pouze pacient s elektronickou identitou bude moci přímo konzumovat služby EZ. Pacienti bez elektronické identity budou služby konzumovat nepřímo přes zdravotnické pracovníky. Cílem je využít stávajících procesů a prostředků eGovernmentu k přihlašování (autentizaci) ke službám EZ určených pro pacienty a definovat různé požadované minimální úrovně důvěry pro různé služby EZ. Autentizační mechanismus pro osoby nevedené v základním registru obyvatel bude navržen zákonem tak, aby tyto osoby mohly mít přístup k vybraným službám EZ (vstup přes portál elektronického zdravotnictví a čerpání jeho informačních služeb, vedení osobního zdravotního záznamu jako volitelné služby). Při návštěvě lékaře nedochází k elektronické identifikaci, dochází k fyzické identifikaci na základě průkazu totožnosti. Na základě průkazu totožnosti provede lékař dohledání záznamu v ARP dle identifikačních údajů. V případě, žení záznam nalezen, lékař zakládá nový záznam. Pro přístup ke službám NCP využívá pacient výhradně přihlašování přes NIA. **POPIS VĚCNÉHO ZÁMĚRU** Elektronická identita občana ČR je zajištěna státem dle zákona o elektronické identifikaci. Centrální autoritou zajišťující elektronickou identitu fyzické osoby je MV včetně Správy základních registrů. Systémem zajišťující elektronickou identifikaci je NIA, tento systém slouží jako prostředník mezi poskytovateli identity (ID providery) a poskytovateli služeb (Service providery). U fyzické osoby se předpokládá, že bude mít na výběr z několika poskytovatelů identit, mezi kterými se v rámci nejvyšší úrovně důvěry (LoA vysoká) dá počítat s eOP, tedy nosičem a SW prostředkem garantovaným státem. Ostatní ID provideři zatím nejsou známi, mohou se přihlašovat od 1. 7. 2018. Služby EZ budou moci využít pouze pacienti, kteří budou mít elektronickou identitu na potřebné úrovni důvěry. Ostatní ji nebudou moci využít a do

	systému budou vstupovat jen nepřímo prostřednictvím zdravotnických pracovníků. Při prezenčním prokázání identity (v ordinaci, lékárně apod.) budou nadále zachovány stávající procesy a úroveň důvěry mezi lékařem a pacientem s výjimkou prokazování identity nových neznámých osob. V tomto případě je vyžadováno prokazování identity na základě OP. V případě cizinců pak jiné identifikační prostředky stanovené vyhláškou. Pro elektronickou formu prokázání identity je nutné myslet na integraci prostředků pro elektronickou identifikaci se systémy PZS. Důležitým faktem hodným zřetele je, že kartička pojištěnce neobsahuje část pro uložení SW prostředku pro prokázání identity. Je tedy nevhodné, aby v současné podobě sloužila jako spolehlivý prostředek prezenčního prokázání totožnosti, neboť nenese sama o sobě žádný údaj potvrzující oprávněnost držitele (fotografie). Buď bude nahrazena pro prezenční prokázání totožnosti jiným dokladem, nebo je nutné provést změny nejen ve vzhledu, ale i funkčnosti a uložit toto ZP. Toto opatření ale vyvolá redundantní pořizovací a udržovací náklady. Za systémové považujeme využití eOP i pro prezenční prokázání identity. Pro prokazování identity nebude karta pojištěnce používána, protože neobsahuje základní prvky identifikace jako např. fotografii. Její využití bude přirozeně ustupovat s náběhem centrálních autentizačních služeb a fungujícího ARP, který určí příslušnost k ZP. Tímto postupem není dotčena ta skutečnost, že pro čistě prezenční prokázání lze užít jakoukoliv veřejnou listinu s fotografií, to ale tento zákon neřeší. Pro účely utajení činnosti zpravodajských služeb České republiky, Policie České republiky, Celní správy České republiky a Generální inspekce bezpečnostních sborů a zajištění bezpečnosti jejich příslušníků se počítá s použitím zvláštních postupů.

Element Řízení identit Zdravotnických Pracovníků

Typ	ApplicationFunction
Popis	**ÚČEL** Klíčovou podmínkou pro rozvoj elektronizace je existence elektronické identity zdravotnických pracovníků. Zdravotnický pracovník bude přistupovat formou dálkového přístupu k centrálním službám elektronického zdravotnictví: • U větších PZS prostřednictvím infomačních systémů PZS, ke kterým bude zdravotnický pracovník přistupovat (bude se autentizovat) na základě identitního prostředku vydaného a spravovaného poskytovatelem zdravotních služeb. Tato praxe je dnes v nemocnicích běžně zavedena. Do budoucna budou tyto autentizační prostředky odpovídat standardu vydaného Národním centrem pro elektronické zdravotnictví v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a změně některých zákonů (zákon o kybernetické bezpečnosti a jeho prováděcí vyhlášky č. 82/2018 Sb., o kybernetické

bezpečnosti.

- V primární sféře kde PZS žádné identitní prostředky nevydává, budou provozovatelem IDDR (ÚZIS) vydávány systémové certifikáty pro přístup do centrálních služeb. Samotné přihlašování do užívaných ambulantních systémů (PC Doktor, apod.) bude vytvářeno ve spolupráci s dodavateli těchto systémů. Provozovatel IDDR může vydávat a spravovat používané přihlašovací prostředky.
- Pro ověření identity budou respektováni poskytovatelé identity uvedení v oznámeném identitním schématu ČR a dle nařízení v rámci systému eIDAS a na odpovídajícím stupni důvěry definovaným v souladu s příslušnou vyhláškou.

Od července 2018 je v účinnosti zákon č. 250/2017 Sb., o elektronické identifikaci (dále jen „zákon o elektronické identifikaci“), který řeší zavedení identit občanů, zajištění požadovaných úrovní záruky, garance procesů prokazování a ověřování totožnosti a vydávání prostředků pro elektronickou identifikaci a řadu technických a bezpečnostních požadavků a související státem provozovanou infrastrukturu.

Požadovanou úroveň důvěry pro vybrané typy identitních služeb bude tedy třeba definovat i s přihlédnutím na probíhající aktivity na úrovni EU, které revidují požadavky na úroveň zabezpečení identity ve vztahu k poskytovaným službám EZ. Tímto přístupem bude zajištěna i potřebná časová a legislativní pružnost v případě potřeby operativně změnit nastavení požadovaných úrovní důvěry vyvolaná na národní či evropské úrovni, která by cestou novelizace zákona trvala mnohem déle.

Požadovaná úroveň záruky

Citlivá zdravotnická data, resp. zvláštní kategorie osobních údajů, je třeba chránit prostředky pro identifikaci s dostatečnou úrovní záruky. Pracují-li zdravotničtí pracovníci převážně se zvláštními kategoriemi osobních údajů, je zapotřebí zajistit zabezpečený přístup k těmto datům. Z tohoto pohledu je třeba vzít v potaz hranici minimálního rizika a zaručit **dostatečnou úroveň záruky** prostředku pro identifikaci. Požadovaný stupeň důvěry a odpovídající autentizační prostředky pro přístup k jednotlivým centrálním službám EZ **určí správce těchto služeb** podle míry souvisejícího rizika.

POPIS VĚCNÉHO ZÁMĚRU

Legislativní opatření umožní jednotlivým subjektům používat navržené procesy autentizace a autorizace. Identifikační prostředek pro prokázání identity (certifikát) si bude moci zdravotnický pracovník zvolit; předpokládá se, že kromě centrální rezortní autority budou dostupné i komerční certifikáty od soukromých organizací splňující podmínky NIA. Systém bude otevřený i pro budoucí profesní karty. Profesní karty jsou variantou, která

	má značné náklady a je potřeba dohodnout proces jejich vydávání, obsluhy a také zavedení do praxe, aby nebyli zatíženi zdravotničtí pracovníci. Z pohledu mnoha nevyjasněných připomínek bylo od zařazení profesních karet prozatím upuštěno. Proces elektronické identifikace zdravotnického pracovníka se (jako v každém jiném oboru) skládá z identifikace, autentizace a autorizace. Identifikace a autentizace je zprostředkována identifikačním prostředkem pro prokázání a ověření identity u každé fyzické osoby v roli zdravotnického pracovníka. Proces autentizace bude využívat i data z ARZP, a to zejména v případech, kdy zdravotnický pracovník nebude nalezen v základním registru obyvatel, ani v agendovém informačním systému cizinců. Pro identifikaci a autentizaci zdravotnického pracovníka bude vyžadován identifikační prostředek úrovní důvěry definovanou poskytovatelem elektronické služby v souladu s příslušnou vyhláškou. Autorizaci neboli správné obsazení zdravotnického pracovníka do role (například lékař v definovaném oboru s příslušnou atestací, lékař v roli revizního lékaře apod.), potřebnou pro přístup do jednotlivých IS, poskytne zdroj autoritativních údajů – ARZP. **Navrhovaný způsob pořizování prostředků elektronické identifikace** Prostřednictvím IDRR infrastruktury budou moci být vydávány zdravotnickým pracovníkům rezortní identifikační certifikáty MZ, které mohou být jedním z autentizačních prostředků umožňující přístup zdravotnického pracovníka k centrálním službám EZ. PZS mohou v rámci svých procesů tento certifikát umístit na nosič (například kartu) a využít pro autentizaci v rámci zdravotnického zařízení. Prostředek pro prokázání identity si bude moci zdravotnický pracovník zvolit; předpokládá se, že kromě zmíněných státem vydaných autentizačních certifikátů budou dostupné i komerční prostředky od soukromých organizací identitních prostředků splňující podmínky NIA . Těmito prostředky pro autentizaci by mohly být karty s certifikáty poskytovanými již nyní lékařům v nemocnicích, kde jednotliví PZS mají uzavřeny komerční smlouvy s poskytovateli kvalifikovaných certifikátů a tito tak mají v nemocnicích své pobočky pro vydávání certifikátů lékařům. Je jistě velmi účelné, aby se tato místa (kontaktní body certifikačních autorit), která vznikají již nyní, využila i pro vydávání certifikátů pro účely identifikace, podepisování či šifrování. Podmínkou využití autentizace prostřednictvím NIA je evidence dané osoby v základním registru obyvatel. Pro zahraniční pracovníky, kteří nejsou evidováni v základním registru obyvatel, je proto nutné aktivovat tzv. evidenci jiných fyzických osob (AJFO) ve smyslu § 17 písm. e) zákona o základních registrech. Proces autentizace a identifikace předpokládá mimo jiné plně funkční infrastrukturní služby resortu zdravotnictví (především fungující

	komponenty IDRR), které poskytuje službu autorizace pro ověření role zdravotnického pracovníka pomocí autoritativních registrů a RPM. Předpoklady: • Bude plně funkční ARZP a procesy jeho aktualizace a správy. • Zdravotnickému pracovníkovi bude umožněno využívání služeb eGovernmentu (autentizace prostřednictvím NIA). V případech, kdy nebude národní bod pro identifikaci a autentizaci či autentizační server dostupný, nebude autentizace zdravotnického pracovníka prostřednictvím NIA možná. Nicméně vzhledem k tomu, že téměř všechna komunikace bude probíhat přes systémy poskytovatelů mimo NIA, není krátkodobá nedostupnost NIA reálně v tomto směru kritická pro poskytování zdravotních služeb.

Element Řízení oprávnění přístupů ke službám

Typ	ApplicationComponent
Popis	Komponenta IAM, zajišťující řízení (nastavení) oprávnění přístupu subjektů ke službám elektronického zdravotnictví. Obsahuje: • Matici: Subjekt + Agenda + ISSubjektu / Služba • Workflow pro schvalování rolí a oprávnění **Matice: Subjekt + Agenda + ISSubjektu / Služba** Tato komponenta obsahuje vztahy mezi: 1. Subjekty - tedy zdravotnický pracovník, poskytovatel zdravotních služeb, pracoviště, zařízení nebo jiná část PZS 2. Agenda elektronického zdravotnictví - tedy věcnou oblast elektronického zdravotnictví 3. IS Subjektu - tedy informační systémy subjektu vstupujícího do elektronického zdravotnictví (jeden subjekt může mít více systémů, které vstupují do EZ) 4. Opr8vnění na užití služby EZ - tedy služby poskytované prostřednictvím IDRR klientům (tedy zejména poskytovatelům zdravotních služeb) **Nastavení oprávnění** Záznamy do matice oprávnění provádí správce IAM prostřednictvím služby Nastavení přístupových oprávnění. **Kontrola oprávnění** Funkce Matice spočívá v tom, že pro daný Subjekt, vykonávanou agendu a použitý informační systém podá seznam služeb elektronického zdravotnictví, které může subjekt v dané agendě a IS využívat (volat). Tato funkce je spuštěna voláním služby Kontrola přístupových oprávnění. V případě, že pro danou kombinaci neexistuje záznam v matici služba,

	kontrola přístupových oprávnění poskytne prázdný seznam služeb.

Element ROB

Typ	ApplicationComponent
Popis	**Registr obyvatel** Subjekty údajů vedených v registru obyvatel jsou a) státní občané České republiky, b) cizinci, kteří pobývají na území České republiky v rámci trvalého pobytu anebo na základě dlouhodobého víza nebo povolení k dlouhodobému pobytu, c) občané jiných členských států Evropské unie, občané států, které jsou vázány mezinárodní smlouvou sjednanou s Evropským společenstvím, a občané států, které jsou vázány smlouvou o Evropském hospodářském prostoru, a jejich rodinní příslušníci, kteří pobývají na území České republiky v rámci trvalého pobytu nebo kterým byl vydán doklad o přechodném pobytu na území České republiky delším než 3 měsíce, d) cizinci, kterým byla na území České republiky udělena mezinárodní ochrana formou azylu nebo doplňkové ochrany11), e) jiné fyzické osoby, u nichž jiný právní předpis vyžaduje agendový identifikátor fyzické osoby a stanoví, že tyto fyzické osoby budou vedeny v registru obyvatel.

Element Role pro oprávnění přístupu k Zdravotnické dokumentaci a Autoritativním údajům

Typ	DataObject
Popis	Role pro oprávnění přístupu k Zdravotnické dokumentaci a Autoritativním údajům.

Element Rozhraní na ISZR

Typ	ApplicationInterface
Popis	Rozhraní RDR, na kterém jsou vystaveny služby pro integraci s Informačním Systémem Základních registrů, čímž zajišťuje volání dílčích služeb Základních registrů Obyvatel, Osob, Územní Identifikace a Práv a Povinností pro potřeby systému IDRR.

Element Služba zprostředkující ověření identity a poskytnutí atributů osob

Typ	ApplicationService
Popis	Služba zprostředkující ověření identity a poskytnutí atributů osoby za účelem jejího jednoznačného ztotožnění. Osobou u níž je identita ověřována může být Pacient nebo Zdravotnický pracovník.

Element Služby elektronického zdravotnictví

Typ	DataObject
Popis	Služby elektronického zdravotnictví

Element Služby kontroly přístupových oprávnění

Typ	ApplicationService
Popis	Služby kontroly přístupových oprávnění poskytuje subsystém pro správu identit a oprávnění (IAM) dalším subsystémům IDRR, za účelem řízeného přístupu k údajům v nich vedených.

Element Služby ověření oprávnění a udílení mandátů

Typ	ApplicationService
Popis	Skupina služeb **ověření oprávnění a udílení mandátů** zajišťuje udělení, ověření a zrušení mandátu pro zastupování pacienta a oprávnění pro nakládání s jeho Zdravotnickou dokumentací formou souhlasu pacienta. Tyto služby poskytuje subsystém Registru práv a mandátů a jsou zprostředkované pro další subsystémy Rezortním Datovým Rozhraním (RDR)

Element Služby poskytování autoritativních údajů

Typ	ApplicationService
Popis	Služby pro poskytování autoritativních údajů systémem ISAR.

Element Služby pro komunikaci IDRR se systémy eGOV

Typ	ApplicationService
Popis	Služby IDRR pro komunikaci se systémy eGovernmentu zajišťuje Rezortní Datové Rozhraní (RDR), které je zprostředkovává pro dílčí subsystémy IDRR, především pro tři Autoritativní Registry.

Element Služby ztotožnění osob

Typ	ApplicationService
Popis	Služby subsystému správy identit a oprávnění (IAM) pro ztotožnění identity osoby, které potřebují další subsystémy IDRR nebo subjekty zdravotnictví ve svých Informačních systémech na lokální úrovni.

Element Služby ztotožnění osob a kontroly přístupových oprávnění

Typ	ApplicationService
Popis	Služby ztotožnění osob a kontroly přístupových oprávnění

Element Správa identit a oprávnění (IAM)

Typ	ApplicationComponent

Popis	IAM, jakožto centrální subsystém IDRR, bude prostřednictvím RDR napojen na NIA, aby mohl volat službu **Ověření identity uživatele centrálních služeb EZ - Pacienta**. Služba **Ověření identity uživatele centrálních služeb EZ - Zdravotníka na požadovanou úroveň záruky**, která má být poskytována plánovaným systémem ověření identit resortních pracovníků (IdRP - MVČR), bude rovněž zprostředkována RDR. IDRR by mělo dále zprostředkovat jednotné napojení na **resortní identitu** (Certifikační autorita - provozovatel ÚZIS) a zajistit tak autorizaci do systémů elektronického zdravotnictví, kterou by využívaly další subjekty resortu. Za účelem sjednocování by měl být IDRR oprávněn (respektive jeho věcný správce) navázat svými **Autoritativními registry** na evidence subjektů (lékařů a PZS) vedených SÚKL v eReceptu, pokud to bude účelné. Reálně se jedná o logické propojení subsystému IAM (IDRR) se systémy eRecept (ŠUKL), prostřednictvím RDR.

Element Správa vydaných identifikačních a autentizačních prostředků (sys cert)

Typ	ApplicationComponent
Popis	Komponenta (IAM), která zajišťuje správu vydaných identifikačních a autentizačních prostředků (sys cert), které ukládá do Dlouhodobého úložiště.

Element Subjekt eZdravotnictví

Typ	DataObject
Popis	Datový objekt, který reprezentuje část matice oprávnění - Subjekt eZdravotnictví.

Element Typy oprávnění a klasifikace ZD

Typ	DataObject
Popis	Typy oprávnění a klasifikace ZD.

Element Typy základních a zákonných zmocnění

Typ	DataObject
Popis	Základní typy zmocnění (např. plynoucí z příbuzenských vztahů Rodič - Dítě, Manžel - Manželka) a zákonné zmocnění (Opatrovník - Dítě)

Element Workflow pro schvalování rolí a oprávnění

Typ	ApplicationFunction

Popis	Funkce zajišťující dodržování přesného metodického a pracovního postupu při žádání, udělování nebo odnímání oprávnění subjektům zdravotnictví pro využívání centrálních služeb elektronického zdravotnictví. Důvodem pro zavedení této podpůrné služby je urychlení procesů správy oprávnění, omezení chybovosti a naprostá transparentnost procesu správy oprávnění ke službám elektronického zdravotnictví, které pracují s osobními a citlivými zdravotnickými informacemi pacientů.

Element Základní registry (ISZR)

Typ	ApplicationComponent
Popis	Základní registry (ISZR)

1.2 Diagram: (AA) eID - autentizace zdravotnického pracovníka

Subsystém – eID - autentizace zdravotnického pracovníka

Účel
Tento diagram zachycuje komponenty, služby a funkce elektronického zdravotnictví pro přístup zdravotnických pracovníků a poskytovatelů zdravotních služeb ke službám elektronického zdravotnictví.

Popis základní funkcionality subsystému
Zdravotnický pracovník má dvě možnosti přístupu ke službám eZ:
1. Prostřednictvím Národního zdravotnického informačního portálu (NZIP)
2. Prostřednictvím systému poskytovatele zdravotních služeb (IS PZS)

Autentizace
Při přístupu ke službám eZ prostřednictvím NZIP využívá část NZIP pro zdravotnické pracovníky. Tato část portálu je neveřejná a vyžaduje autentizaci a autorizaci. Pro autentizaci k NZIP využívá autentizační služby Národní identitní autority (NIA), případně autentizačního prostředku, který získal od MZČR.

Při přístupu prostřednictvím informačního systému poskytovatele zdravotních služeb (IS PZS), se zdravotnický pracovník autentizuje vůči tomuto systému (tedy vůči IS PZS) prostřednictvím lokálního účtu v IAM PZS. Po autentizaci a ověření přístupu může zdravotnický pracovník využívat služby eZ.

Autorizace
Autorizace zdravotnického pracovníka ke službám eZ probíhá v IAM IDRR. Ověřuje se, zda daný zdravotnický pracovník vystupující za poskytovatele zdravotních služeb může přistupovat k datům a službám eZ.

Předpoklady
Východiska
- Existence IAM, resortní certifikační autority

Principy a pravidla
- Autentizace zdravotnického pracovníka buď prostřednictvím NIA, nebo autentizačním prostředkem ÚZIS, nebo prostřednictvím IS PZS

Při přístupu prostřednictvím IS PZS platí, že

- IS PZS musí využívat certifikovaný systém pro přístup k eZ
- IS PZS je zaregistrovaný v IDRR pro přístup ke službám eZ (vlastní systémový certifikát pro připojení k IDRR)
- IS PZS má ztotožněné uživatele vůči IDRR (tedy vůči autoritativnímu registru zdravotnických pracovníků)

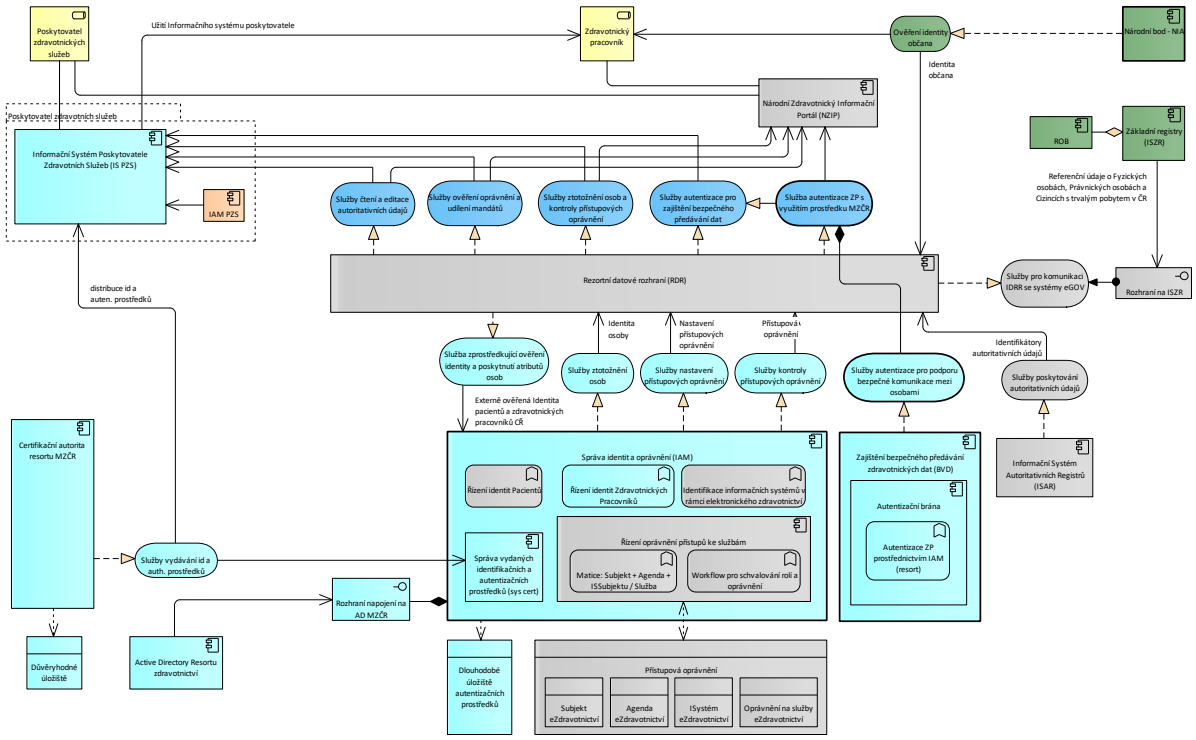
Vazby

Interní

- ARZP - informace o zdravotnickém pracovníkovi
- IAM - autentizace a autorizace zdravotnického pracovníka
- CA MZČR - certifikační autorita MZČR

Externí

- NIA - autentizace občana
- ISZR, ROB - informace o občanovi
- IS PZS - informační systém poskytovatele zdravotních služeb



Element Active Directory Resortu zdravotnictví

Typ	ApplicationComponent
Popis	Aplikační komponenta Active Directory Resortu zdravotnictví

Element Agenda eZdravotnictví

Typ	DataObject
Popis	Datový objekt, který reprezentuje část matice oprávnění - Agendu

	eZdravotnictví.

Element Autentizace ZP prostřednictvím IAM (resort)

Typ	ApplicationFunction
Popis	Autentizace ZP prostřednictvím IAM (resort)

Element Autentizační brána

Typ	ApplicationComponent
Popis	Komponenta subsystému Bezpečného předávání zdravotnických dat zajišťující autentizační služby.

Element Certifikační autorita resortu MZČR

Typ	ApplicationComponent
Popis	Elektronický podpis je nezbytnou součástí systému ochrany před zneužitím údajů ve zdravotnictví a autorizuje obsah podepsaného dokumentu. Měl by být pro všechny sjednocen na stejnou úroveň. Zákon o zdravotních službách v § 54 stanoví povinnost zdravotnického pracovníka nebo jiného odborného pracovníka každý zápis do ZD vedené v elektronické podobě opatřit identifikátorem záznamu; samotný zápis obsahuje nezměnitelné, nezpochybnitelné a ověřitelné údaje, kterými jsou datum provedení zápisu a identifikační údaje zdravotnického pracovníka nebo jiného odborného pracovníka, který záznam provedl. Například elektronická preskripce elektronický podpis vyžaduje při každé aktivní operaci – vystavení, opravě eReceptu, výdeji, opravě výdeje eReceptu. eIDAS uvádí: • Nutnost využít pro kvalifikovaný podpis kvalifikovaného prostředku. • Kvalifikovaný prostředek je certifikovaný podle příslušných technických norem uvedených v prováděcím rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a je uveden v seznamu kvalifikovaných prostředků. Z § 5 a § 6 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, (dále jen „zákon o službách vytvářejících důvěru pro elektronické transakce“) navazujícího na výše uvedené nařízení Evropského parlamentu a Rady (EU) vyplývá, že: • Veřejnoprávní podepisující (což zdravotnický pracovník při poskytování zdravotních služeb není) musí od 19. září 2018 k podepisování elektronickým podpisem (podepisuje-li elektronický dokument, kterým právně jedná) použít pouze kvalifikovaný elektronický podpis. • Od 19. září 2018 musí celá veřejná správa používat pouze: kvalifikované

	elektronické podpisy, kvalifikované elektronické pečeti a kvalifikovaná elektronická časová razítka • Kvalifikovaný elektronický podpis, pečeť či časové razítko musí být založen na kvalifikovaném elektronickém prostředku nebo kvalifikované službě. MV ve svých metodických materiálech uvádí, že kvalifikovaní poskytovatelé služeb vytvářejících důvěru oznamují MV prostředky, na které certifikát pro kvalifikovaný podpis elektronický podpis vydávají. Z hlediska dostupnosti prostředků pro vytváření kvalifikovaného podpisu se v ČR nyní obecně liší PZS - lůžkové a nelůžkové péče. Většina lůžkových PZS v ČR (převážně velcí a střední PZS) se rozhodla vybavit své zaměstnance prostředky pro vytváření kvalifikovaného podpisu na bázi **kvalifikovaného prostředku** a odpovídajícího certifikátu. Jedná se o elektronický podpis **s nejvyšší mírou důvěry**. PZS takto ve velké míře vybavila pouze ty zaměstnance, kteří provádějí ePreskripci. Naopak většina zdravotníků nelůžkových PZS, zejména v primární péči, zachovala **pouze zaručený elektronický podpis** založený na kvalifikovaném certifikátu pro elektronický podpis. Jedná se o elektronický podpis založený na certifikátu, který je vydán akreditovanou certifikační autoritou, ale není povinností klíč certifikátu uložit do kvalifikovaného prostředku. Certifikáty jsou v obou případech vydávány certifikovanými institucemi za poplatek s omezenou roční platností. Ve zdravotnictví působí PZS, která budou v některých případech jednat jako veřejnoprávní instituce (veřejnoprávní podepisující dle § 5 zákona o službách vytvářejících důvěru pro elektronické transakce), které musí při podepisování dokumentů, kterým se právně jedná, používat kvalifikovaný elektronický podpis. Citace ze zákona: „K podepisování elektronickým podpisem lze použít pouze kvalifikovaný elektronický podpis, podepisuje-li elektronický dokument, kterým právně jedná, a) stát, územní samosprávný celek, právnická osoba zřízená zákonem nebo právnická osoba zřízená nebo založená státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem (dále jen "veřejnoprávní podepisující"), nebo b) osoba neuvedená v písmenu a) při výkonu své působnosti.“ Zároveň ve zdravotnictví působí i jiní PZS zřízené fyzickou či právnickou osobou. Bylo by vhodné, stejně jako v případě identifikace, pracovat na sjednocení úrovně elektronického podpisu napříč PZS ve zdravotnictví a stanovení závazných pravidel pro používání úrovně elektronického podpisu v situacích, kdy se nejedná o právní jednání. Závěr k elektronickému podpisu: Zákon zavede možnost vydávat a využívat rezortní prostředky s vysokou nebo značnou úrovní záruky pro elektronický

	podpis, které mohou být uznávány dalšími rezorty, kde to bude vhodné (MPSV, ČSSZ). Zároveň umožní dále využívat i dostupné a v praxi rozšířené kvalifikované prostředky pro elektronický podpis.

Element Dlouhodobé úložiště autentizačních prostředků

Typ	DataObject
Popis	Dlouhodobé úložiště a evidence vydaných autentizačních prostředků subjektům zdravotnictví.

Element Důvěryhodné úložiště

Typ	DataObject
Popis	Důvěryhodné úložiště Certifikační autority MZČR.

Element IAM PZS

Typ	ApplicationComponent
Popis	Systém poskytovatele zdravotních služeb, který zajišťuje autentizaci a správu přístupů zdravotnických pracovníků k informačnímu systému poskytovatele zdravotních služeb.

Element Identifikace informačních systémů v rámci elektronického zdravotnictví

Typ	ApplicationFunction
Popis	**ÚČEL** V tomto případě se nejedná o ztotožňování osob, ale o identifikaci a ztotožnění informačních systémů. Tato identifikace a ztotožnění v praxi představuje autentizační prostředek - systémový certifikát - vydávaný Certifikační autoritou resortu jednotlivým subjektům elektronického zdravotnictví **pro účely zabezpečení komunikace** při volání Centrálních služeb EZ.

Element Informační Systém Autoritativních Registrů (ISAR)

Typ	ApplicationComponent
Popis	Informační Systém Autoritativních Registrů (ISAR) zajišťuje společné funkce pro dílčí autoritativní registry: • Autoritativní registr pacientů (ARP) • Autoritativní registr zdravotnických pacientů (ARZP) • Autoritativní registr poskytovatelů zdravotních služeb (ARPZS) a připojení těchto registrů na Rezortní Datové Rozhraní prostřednictvím služeb pro Poskytování a Editaci autoritativních údajů.

Element Informační Systém Poskytovatele Zdravotních Služeb (IS PZS)

Typ	ApplicationComponent

Popis	Informační systém poskytovatele zdravotních služeb, kterým přistupuje k centrálním službám elektronického zdravotnictví. Z pohledu lokálního lékaře se dále jedná o systémy, které vedou dle platné legislativy Zdravotnickou dokumentaci pacienta, kterou jsou schopny poskytnout jako záznamy prostřednictvím rozhraní (v případě OpenNCPe ve formátu MeDocs).

Element ISystém eZdravotnictví

Typ	DataObject
Popis	Datový objekt, který reprezentuje část matice oprávnění - Informační systém elektronického zdravotnictví.

Element Matice: Subjekt + Agenda + ISSubjektu / Služba

Typ	ApplicationFunction
Popis	Funkce pro vložení, změnu a výmaz záznamu v matice oprávnění IAM, který je tvořen údaji: **Subjekt + Agenda + ISSubjektu** pro danou **Centrální službu elektronického zdravotnictví.** Tímto záznamem oprávnění je jednoznačně definován přístup k množině služeb pro využití konkrétním subjektem při výkonu agendy a za použití stanoveného informačního subjektu

Element Národní bod - NIA

Typ	ApplicationComponent
Popis	Národní bod pro identifikaci, někdy též Národní identitní autorita (NIA) umožňuje autentizaci občanů a ověření identity pro následné využívání elektronických služeb státu. Občan si může vybírat z různých autentizačních služeb (eOP, Jméno+heslo+SMS, v budoucnu též bankovní ID). Pro oblast zdravotnictví se bude plně využívat těchto státem garantovaných a poskytovaných služeb pro roli Pacient.

Element Národní Zdravotnický Informační Portál (NZIP)

Typ	ApplicationComponent
Popis	Portál zajišťuje vizuální rozhraní pro veřejnost, pacienty a pojištěnce, zdravotnické pracovníky, pověřené osoby, správce provozu a řízení tvorby obsahu portálu. NZIP je komponenta, která se podílí hlavní měrou na naplnění Strategického cíle 1: Zvýšení zainteresovanosti občana na péči o vlastní zdraví. Zahrnuje procesy • strategické řízení NZIP,

	• zdroje a financování, • řízení vztahů s partnery, • vlastní proces tvorby obsahu NZIP, • poskytování informací anonymnímu uživateli i uživatelům oprávněným (registrovaným), • zajištění technické správy a provozu.

Element Oprávnění na služby eZdravotnictví

Typ	DataObject
Popis	Datový objekt, který obsahuje persistentně uložený záznam oprávnění subjektu, agendy a informačního systému pro užití vybrané množiny služeb elektronického zdravotnictví.

Element Ověření identity občana

Typ	ApplicationService
Popis	Služba veřejné správy zajišťující ověření identity občana nebo cizince žijícího v České republice.

Element Poskytovatel zdravotních služeb

Typ	Grouping
Popis	Perimetr poskytovatele zdravotních služeb.

Element Poskytovatel zdravotnických služeb

Typ	BusinessRole
Popis	Role Poskytovatel zdravotnických služeb přistupuje k využívání centrálních služeb eZdravotnictví výhradně na základě oprávnění a jednoznačné identifikace subjektu a jeho zaměstnanců. Přístup k centrálním službám elektronického zdravotnictví je možný dvojím způsobem: prostřednictvím vizuálního rozhraní Národního Zdravotního Informačního Portálu (NZIP) a **prostřednictvím Informačního Systému Poskytovatele Zdravotních Služeb (ISPZS)**, který je integrován na systém Rezortní Datové Rozhraní (RDR) a tvoří základ služeb pro PZS z dílčích služeb vybraných subsystémů IDRR.

Element Přístupová oprávnění

Typ	DataObject
Popis	Datové úložiště relační databáze, které zajišťuje persistentní uložení přístupových oprávnění pro užití služeb elektronického zdravotnictví pro dané subjekty a agendy vykonávané ve zdravotnictví.

Element Rezortní datové rozhraní (RDR)

Typ	ApplicationComponent

Popis	Resortní datové rozhraní představují klíčovou komponenty IDRR, která je Integrační platformou pro subsystémy IDRR.

Element Řízení identit Pacientů

Typ	ApplicationFunction
Popis	**ÚČEL** Zajistit identifikaci a autentizaci pacienta neboli ověření a garantování identity pro přístup a využívání služeb EZ. Daný způsob nemusí být určen čistě pro elektronické služby, ale může být využit i při asistovaném způsobu využívání služeb, např. povolení k náhledu do ZD při fyzické návštěvě zdravotnického pracovníka. Pouze pacient s elektronickou identitou bude moci přímo konzumovat služby EZ. Pacienti bez elektronické identity budou služby konzumovat nepřímo přes zdravotnické pracovníky. Cílem je využít stávajících procesů a prostředků eGovernmentu k přihlašování (autentizaci) ke službám EZ určených pro pacienty a definovat různé požadované minimální úrovně důvěry pro různé služby EZ. Autentizační mechanismus pro osoby nevedené v základním registru obyvatel bude navržen zákonem tak, aby tyto osoby mohly mít přístup k vybraným službám EZ (vstup přes portál elektronického zdravotnictví a čerpání jeho informačních služeb, vedení osobního zdravotního záznamu jako volitelné služby). Při návštěvě lékaře nedochází k elektronické identifikaci, dochází k fyzické identifikaci na základě průkazu totožnosti. Na základě průkazu totožnosti provede lékař dohledání záznamu v ARP dle identifikačních údajů. V případě, žení záznam nalezen, lékař zakládá nový záznam. Pro přístup ke službám NCP využívá pacient výhradně přihlašování přes NIA. **POPIS VĚCNÉHO ZÁMĚRU** Elektronická identita občana ČR je zajištěna státem dle zákona o elektronické identifikaci. Centrální autoritou zajišťující elektronickou identitu fyzické osoby je MV včetně Správy základních registrů. Systémem zajišťující elektronickou identifikaci je NIA, tento systém slouží jako prostředník mezi poskytovateli identity (ID providery) a poskytovateli služeb (Service providery). U fyzické osoby se předpokládá, že bude mít na výběr z několika poskytovatelů identit, mezi kterými se v rámci nejvyšší úrovně důvěry (LoA vysoká) dá počítat s eOP, tedy nosičem a SW prostředkem garantovaným státem. Ostatní ID provideři zatím nejsou známi, mohou se přihlašovat od 1.

	7. 2018. Služby EZ budou moci využít pouze pacienti, kteří budou mít elektronickou identitu na potřebné úrovni důvěry. Ostatní ji nebudou moci využít a do systému budou vstupovat jen nepřímo prostřednictvím zdravotnických pracovníků. Při prezenčním prokázání identity (v ordinaci, lékárně apod.) budou nadále zachovány stávající procesy a úroveň důvěry mezi lékařem a pacientem s výjimkou prokazování identity nových neznámých osob. V tomto případě je vyžadováno prokazování identity na základě OP. V případě cizinců pak jiné identifikační prostředky stanovené vyhláškou. Pro elektronickou formu prokázání identity je nutné myslet na integraci prostředků pro elektronickou identifikaci se systémy PZS. Důležitým faktem hodným zřetele je, že kartička pojištěnce neobsahuje část pro uložení SW prostředku pro prokázání identity. Je tedy nevhodné, aby v současné podobě sloužila jako spolehlivý prostředek prezenčního prokázání totožnosti, neboť nenese sama o sobě žádný údaj potvrzující oprávněnost držitele (fotografie). Buď bude nahrazena pro prezenční prokázání totožnosti jiným dokladem, nebo je nutné provést změny nejen ve vzhledu, ale i funkčnosti a uložit toto ZP. Toto opatření ale vyvolá redundantní pořizovací a udržovací náklady. Za systémové považujeme využití eOP i pro prezenční prokázání identity. Pro prokazování identity nebude karta pojištěnce používána, protože neobsahuje základní prvky identifikace jako např. fotografii. Její využití bude přirozeně ustupovat s náběhem centrálních autentizačních služeb a fungujícího ARP, který určí příslušnost k ZP. Tímto postupem není dotčena ta skutečnost, že pro čistě prezenční prokázání lze užít jakoukoliv veřejnou listinu s fotografií, to ale tento zákon neřeší. Pro účely utajení činnosti zpravodajských služeb České republiky, Policie České republiky, Celní správy České republiky a Generální inspekce bezpečnostních sborů a zajištění bezpečnosti jejich příslušníků se počítá s použitím zvláštních postupů.

Element Řízení identit Zdravotnických Pracovníků

Typ	ApplicationFunction
Popis	**ÚČEL** Klíčovou podmínkou pro rozvoj elektronizace je existence elektronické identity zdravotnických pracovníků. Zdravotnický pracovník bude přistupovat formou dálkového přístupu k centrálním službám elektronického zdravotnictví: • U větších PZS prostřednictvím infomačních systémů PZS, ke kterým bude zdravotnický pracovník přistupovat (bude se autentizovat) na základě identitního prostředku vydaného a spravovaného poskytovatelem zdravotních služeb. Tato praxe je dnes v nemocnicích běžně zavedena. Do budoucna budou tyto autentizační prostředky odpovídat standardu vydaného Národním centrem pro elektronické

zdravotnictví v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a změně některých zákonů (zákon o kybernetické bezpečnosti a jeho prováděcí vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti.

- V primární sféře kde PZS žádné identitní prostředky nevydává, budou provozovatelem IDDR (ÚZIS) vydávány systémové certifikáty pro přístup do centrálních služeb. Samotné přihlašování do užívaných ambulantních systémů (PC Doktor, apod.) bude vytvářeno ve spolupráci s dodavateli těchto systémů. Provozovatel IDDR může vydávat a spravovat používané přihlašovací prostředky.
- Pro ověření identity budou respektováni poskytovatelé identity uvedení v oznámeném identitním schématu ČR a dle nařízení v rámci systému eIDAS a na odpovídajícím stupni důvěry definovaným v souladu s příslušnou vyhláškou.

Od července 2018 je v účinnosti zákon č. 250/2017 Sb., o elektronické identifikaci (dále jen „zákon o elektronické identifikaci“), který řeší zavedení identit občanů, zajištění požadovaných úrovní záruky, garance procesů prokazování a ověřování totožnosti a vydávání prostředků pro elektronickou identifikaci a řadu technických a bezpečnostních požadavků a související státem provozovanou infrastrukturu.

Požadovanou úroveň důvěry pro vybrané typy identitních služeb bude tedy třeba definovat i s přihlédnutím na probíhající aktivity na úrovni EU, které revidují požadavky na úroveň zabezpečení identity ve vztahu k poskytovaným službám EZ. Tímto přístupem bude zajištěna i potřebná časová a legislativní pružnost v případě potřeby operativně změnit nastavení požadovaných úrovní důvěry vyvolaná na národní či evropské úrovni, která by cestou novelizace zákona trvala mnohem déle.

Požadovaná úroveň záruky

Citlivá zdravotnická data, resp. zvláštní kategorie osobních údajů, je třeba chránit prostředky pro identifikaci s dostatečnou úrovní záruky. Pracují-li zdravotničtí pracovníci převážně se zvláštními kategoriemi osobních údajů, je zapotřebí zajistit zabezpečený přístup k těmto datům. Z tohoto pohledu je třeba vzít v potaz hranici minimálního rizika a zaručit **dostatečnou úroveň záruky** prostředku pro identifikaci. Požadovaný stupeň důvěry a odpovídající autentizační prostředky pro přístup k jednotlivým centrálním službám EZ **určí správce těchto služeb** podle míry souvisejícího rizika.

POPIS VĚCNÉHO ZÁMĚRU

Legislativní opatření umožní jednotlivým subjektům používat navržené procesy autentizace a autorizace. Identifikační prostředek pro prokázání identity (certifikát) si bude moci zdravotnický pracovník zvolit; předpokládá

	se, že kromě centrální rezortní autority budou dostupné i komerční certifikáty od soukromých organizací splňující podmínky NIA. Systém bude otevřený i pro budoucí profesní karty. Profesní karty jsou variantou, která má značné náklady a je potřeba dohodnout proces jejich vydávání, obsluhy a také zavedení do praxe, aby nebyli zatíženi zdravotničtí pracovníci. Z pohledu mnoha nevyjasněných připomínek bylo od zařazení profesních karet prozatím upuštěno. Proces elektronické identifikace zdravotnického pracovníka se (jako v každém jiném oboru) skládá z identifikace, autentizace a autorizace. Identifikace a autentizace je zprostředkována identifikačním prostředkem pro prokázání a ověření identity u každé fyzické osoby v roli zdravotnického pracovníka. Proces autentizace bude využívat i data z ARZP, a to zejména v případech, kdy zdravotnický pracovník nebude nalezen v základním registru obyvatel, ani v agendovém informačním systému cizinců. Pro identifikaci a autentizaci zdravotnického pracovníka bude vyžadován identifikační prostředek úrovní důvěry definovanou poskytovatelem elektronické služby v souladu s příslušnou vyhláškou. Autorizaci neboli správné obsazení zdravotnického pracovníka do role (například lékař v definovaném oboru s příslušnou atestací, lékař v roli revizního lékaře apod.), potřebnou pro přístup do jednotlivých IS, poskytne zdroj autoritativních údajů – ARZP. **Navrhovaný způsob pořizování prostředků elektronické identifikace** Prostřednictvím IDRR infrastruktury budou moci být vydávány zdravotnickým pracovníkům rezortní identifikační certifikáty MZ, které mohou být jedním z autentizačních prostředků umožňující přístup zdravotnického pracovníka k centrálním službám EZ. PZS mohou v rámci svých procesů tento certifikát umístit na nosič (například kartu) a využít pro autentizaci v rámci zdravotnického zařízení. Prostředek pro prokázání identity si bude moci zdravotnický pracovník zvolit; předpokládá se, že kromě zmíněných státem vydaných autentizačních certifikátů budou dostupné i komerční prostředky od soukromých organizací identitních prostředků splňující podmínky NIA . Těmito prostředky pro autentizaci by mohly být karty s certifikáty poskytovanými již nyní lékařům v nemocnicích, kde jednotliví PZS mají uzavřeny komerční smlouvy s poskytovateli kvalifikovaných certifikátů a tito tak mají v nemocnicích své pobočky pro vydávání certifikátů lékařům. Je jistě velmi účelné, aby se tato místa (kontaktní body certifikačních autorit), která vznikají již nyní, využila i pro vydávání certifikátů pro účely identifikace, podepisování či šifrování. Podmínkou využití autentizace prostřednictvím NIA je evidence dané osoby v základním registru obyvatel. Pro zahraniční pracovníky, kteří nejsou evidováni v základním registru obyvatel, je proto nutné aktivovat tzv. evidenci jiných fyzických osob (AJFO) ve smyslu § 17 písm. e) zákona o základních registrech.

	Proces autentizace a identifikace předpokládá mimo jiné plně funkční infrastrukturní služby resortu zdravotnictví (především fungující komponenty IDRR), které poskytuje službu autorizace pro ověření role zdravotnického pracovníka pomocí autoritativních registrů a RPM. Předpoklady: • Bude plně funkční ARZP a procesy jeho aktualizace a správy. • Zdravotnickému pracovníkovi bude umožněno využívání služeb eGovernmentu (autentizace prostřednictvím NIA). V případech, kdy nebude národní bod pro identifikaci a autentizaci či autentizační server dostupný, nebude autentizace zdravotnického pracovníka prostřednictvím NIA možná. Nicméně vzhledem k tomu, že téměř všechna komunikace bude probíhat přes systémy poskytovatelů mimo NIA, není krátkodobá nedostupnost NIA reálně v tomto směru kritická pro poskytování zdravotních služeb.

Element Řízení oprávnění přístupů ke službám

Typ	ApplicationComponent
Popis	Komponenta IAM, zajišťující řízení (nastavení) oprávnění přístupu subjektů ke službám elektronického zdravotnictví. Obsahuje: • Matici: Subjekt + Agenda + ISSubjektu / Služba • Workflow pro schvalování rolí a oprávnění **Matice: Subjekt + Agenda + ISSubjektu / Služba** Tato komponenta obsahuje vztahy mezi: 1. Subjekty - tedy zdravotnický pracovník, poskytovatel zdravotních služeb, pracoviště, zařízení nebo jiná část PZS 2. Agenda elektronického zdravotnictví - tedy věcnou oblast elektronického zdravotnictví 3. IS Subjektu - tedy informační systémy subjektu vstupujícího do elektronického zdravotnictví (jeden subjekt může mít více systémů, které vstupují do EZ) 4. Opr8vnění na užití služby EZ - tedy služby poskytované prostřednictvím IDRR klientům (tedy zejména poskytovatelům zdravotních služeb) **Nastavení oprávnění** Záznamy do matice oprávnění provádí správce IAM prostřednictvím služby Nastavení přístupových oprávnění. **Kontrola oprávnění** Funkce Matice spočívá v tom, že pro daný Subjekt, vykonávanou agendu a použitý informační systém podá seznam služeb elektronického

	zdravotnictví, které může subjekt v dané agendě a IS využívat (volat). Tato funkce je spuštěna voláním služby Kontrola přístupových oprávnění. V případě, že pro danou kombinaci neexistuje záznam v matici služba, kontrola přístupových oprávnění poskytne prázdný seznam služeb.

Element ROB

Typ	ApplicationComponent
Popis	**Registr obyvatel** Subjekty údajů vedených v registru obyvatel jsou a) státní občané České republiky, b) cizinci, kteří pobývají na území České republiky v rámci trvalého pobytu anebo na základě dlouhodobého víza nebo povolení k dlouhodobému pobytu, c) občané jiných členských států Evropské unie, občané států, které jsou vázány mezinárodní smlouvou sjednanou s Evropským společenstvím, a občané států, které jsou vázány smlouvou o Evropském hospodářském prostoru, a jejich rodinní příslušníci, kteří pobývají na území České republiky v rámci trvalého pobytu nebo kterým byl vydán doklad o přechodném pobytu na území České republiky delším než 3 měsíce, d) cizinci, kterým byla na území České republiky udělena mezinárodní ochrana formou azylu nebo doplňkové ochrany11), e) jiné fyzické osoby, u nichž jiný právní předpis vyžaduje agendový identifikátor fyzické osoby a stanoví, že tyto fyzické osoby budou vedeny v registru obyvatel.

Element Rozhraní na ISZR

Typ	ApplicationInterface
Popis	Rozhraní RDR, na kterém jsou vystaveny služby pro integraci s Informačním Systémem Základních registrů, čímž zajišťuje volání dílčích služeb Základních registrů Obyvatel, Osob, Územní Identifikace a Práv a Povinností pro potřeby systému IDRR.

Element Rozhraní napojení na AD MZČR

Typ	ApplicationInterface
Popis	Rozhraní subsystému IAM pro napojení na systém Active Directory MZČR

Element Služba autentizace ZP s využitím prostředku MZČR

Typ	ApplicationService
Popis	Služba zprostředkovaná IDRR, která umožňuje autentizaci zdravotnického pracovníka prostřednictvím prostředku, který obdržel od MZČR.

Element Služba zprostředkující ověření identity a poskytnutí atributů osob

Typ	ApplicationService
Popis	Služba zprostředkující ověření identity a poskytnutí atributů osoby za účelem jejího jednoznačného ztotožnění. Osobou u níž je identita ověřována může být Pacient nebo Zdravotnický pracovník.

Element Služby autentizace pro podporu bezpečné komunikace mezi osobami

Typ	ApplicationService
Popis	Skupina autentizačních služeb pro podporu bezpečné komunikace mezi osobami

Element Služby autentizace pro zajištění bezpečného předávání dat

Typ	ApplicationService
Popis	Služby pro zajištění bezpečného předávání dat

Element Služby čtení a editace autoritativních údajů

Typ	ApplicationService
Popis	Služby čtení a editace autoritativních údajů zprostředkované Rezortním Datovým Rozhraním (RDR).

Element Služby kontroly přístupových oprávnění

Typ	ApplicationService
Popis	Služby kontroly přístupových oprávnění poskytuje subsystém pro správu identit a oprávnění (IAM) dalším subsystémům IDRR, za účelem řízeného přístupu k údajům v nich vedených.

Element Služby nastavení přístupových oprávnění

Typ	ApplicationService
Popis	Služby subsystému správy identit a oprávnění (IAM) pro nastavení přístupových oprávnění, které realizuje komponenta Řízení oprávnění přístupu ke službám

Element Služby ověření oprávnění a udílení mandátů

Typ	ApplicationService
Popis	Skupina služeb **ověření oprávnění a udílení mandátů** zajišťuje udělení, ověření a zrušení mandátu pro zastupování pacienta a oprávnění pro nakládání s jeho Zdravotnickou dokumentací formou souhlasu pacienta. Tyto služby poskytuje subsystém Registru práv a mandátů a jsou zprostředkované pro další subsystémy Rezortním Datovým Rozhraním (RDR)

Element Služby poskytování autoritativních údajů

Typ	ApplicationService
Popis	Služby pro poskytování autoritativních údajů systémem ISAR.

Element Služby pro komunikaci IDRR se systémy eGOV

Typ	ApplicationService
Popis	Služby IDRR pro komunikaci se systémy eGovernmentu zajišťuje Rezortní Datové Rozhraní (RDR), které je zprostředkovává pro dílčí subsystémy IDRR, především pro tři Autoritativní Registry.

Element Služby vydávání id a auth. prostředků

Typ	ApplicationService
Popis	Služba certifikační autority resortu MZČR, která zajišťuje vydávání autentizačních prostředků.

Element Služby ztotožnění osob

Typ	ApplicationService
Popis	Služby subsystému správy identit a oprávnění (IAM) pro ztotožnění identity osoby, které potřebují další subsystémy IDRR nebo subjekty zdravotnictví ve svých Informačních systémech na lokální úrovni.

Element Služby ztotožnění osob a kontroly přístupových oprávnění

Typ	ApplicationService
Popis	Služby ztotožnění osob a kontroly přístupových oprávnění

Element Správa identit a oprávnění (IAM)

Typ	ApplicationComponent
Popis	IAM, jakožto centrální subsystém IDRR, bude prostřednictvím RDR napojen na NIA, aby mohl volat službu **Ověření identity uživatele centrálních služeb EZ - Pacienta**. Služba **Ověření identity uživatele centrálních služeb EZ - Zdravotníka na požadovanou úroveň záruky**, která má být poskytována plánovaným systémem ověření identit resortních pracovníků (IdRP - MVČR), bude rovněž zprostředkována RDR. IDRR by mělo dále zprostředkovat jednotné napojení na **resortní identitu** (Certifikační autorita - provozovatel ÚZIS) a zajistit tak autorizaci do systémů elektronického zdravotnictví, kterou by využívaly další subjekty resortu. Za účelem sjednocování by měl být IDRR oprávněn (respektive jeho věcný

	správce) navázat svými **Autoritativními registry** na evidence subjektů (lékařů a PZS) vedených SÚKL v eReceptu, pokud to bude účelné. Reálně se jedná o logické propojení subsystému IAM (IDRR) se systémy eRecept (ŠUKL), prostřednictvím RDR.

Element Správa vydaných identifikačních a autentizačních prostředků (sys cert)

Typ	ApplicationComponent
Popis	Komponenta (IAM), která zajišťuje správu vydaných identifikačních a autentizačních prostředků (sys cert), které ukládá do Dlouhodobého úložiště.

Element Subjekt eZdravotnictví

Typ	DataObject
Popis	Datový objekt, který reprezentuje část matice oprávnění - Subjekt eZdravotnictví.

Element Workflow pro schvalování rolí a oprávnění

Typ	ApplicationFunction
Popis	Funkce zajišťující dodržování přesného metodického a pracovního postupu při žádání, udělování nebo odnímání oprávnění subjektům zdravotnictví pro využívání centrálních služeb elektronického zdravotnictví. Důvodem pro zavedení této podpůrné služby je urychlení procesů správy oprávnění, omezení chybovosti a naprostá transparentnost procesu správy oprávnění ke službám elektronického zdravotnictví, které pracují s osobními a citlivými zdravotnickými informacemi pacientů.

Element Zajištění bezpečného předávání zdravotnických dat (BVD)

Typ	ApplicationComponent
Popis	Bezpečná brána do EU a mezi subjekty eH v ČR

Element Základní registry (ISZR)

Typ	ApplicationComponent
Popis	Základní registry (ISZR)

Element Zdravotnický pracovník

Typ	BusinessRole
Popis	Role Zdravotnický pracovník přistupuje k využívání centrálních služeb eZ výhradně na základě oprávnění a jednoznačné identifikace. Důvodem je poskytování citlivých osobních a zdravotnických informací. Přístup k centrálním službám elektronického zdravotnictví je možný dvojím způsobem: prostřednictvím vizuálního rozhraní Národního Zdravotního Informačního Portálu (NZIP) a prostřednictvím Informačního Systému

	Poskytovatele Zdravotních Služeb (ISPZS), který je integrován na systém Rezortní Datové Rozhraní (RDR) a využívá centrální služby zdravotnictví. Na portálu NZIP se jedná využívání služeb v následujících oblastech: **Zdravotnická dokumentace** • Index zdravotnické dokumentace (IZD) • Emergency záznam pacienta (EMZ) **Elektronické nástroje ordinace** • Nahlížení do zdravotnické dokumentace • Nahlížení a správa autoritativních údajů pacienta • Náhled do ePreskripce, eDispenzace a eNeschopenky • Žádanky na specializovaná vyšetření • Objednávky a rezervace Role Zdravotnický pracovník využívá, mimo služeb na NZIP, i další Centrální služby eZ prostřednictvím Informačního Systému Poskytovatele Zdravotnických Služeb, typicky NIS, u kterého je zaměstnán nebo Ambulantního SW, který používá, pokud je osobou poskytující zdravotnické služby přímo.

Web strategie: http://www.nsez.cz

Citace dle ČSN ISO 690:2011:
MINISTERSTVO ZDRAVOTNICTVÍ ČESKÉ REPUBLIKY. Aktualizace zpracovaných TO-BE modelů EA prioritních opatření, řešení dle akčního plánu elektronizace, eID – Elektronická Identita. Verze 01.01. Praha, 2019. Licencováno pod CC BY 4.0, licenční podmínky dostupné z:
http://creativecommons.org/licenses/by/4.0/.