SU-MD-su_127

Zabezpečenie efektívneho používania služieb ESO1 poskytovateľmi zdravotnej starostlivosti na celom území SR (projekt ESO1 – D)

Obsah

1 Základné informácie
1.1 Prehľad
1.2 Dôvod
1.3 Rozsah
1.4 Použité skratky a značky
2 Manažérske zhrnutie
2.1 Motivácia
2.2 Popis aktuálneho stavu
2.2.1 Legislatíva
2.2.2 Architektúra
2.2.3 Prevádzka
2.3 Alternatívne riešenia identifikácie a autentifikácie pre eZdravie
2.3.2 Možnosti autorizácie
2.3.3 Multikriteriálna analýza
2.3.4 Kombinácie alternatív
2.4 Alternatívne riešenia monitoringu
2.4.1 Alternatíva M-A – „Rozšírenie a zjednotenie logovania IS PZS"
2.4.2 Alternatíva M-B – „Rozšírenie funkcionality komponentu eZdravie o monitoring zariadenia ZPr a kvality pripojenia na eZdravie"
2.4.3 Alternatíva M-C – „Rozšírenie a zjednotenie logovania IS PZS a využívanie VPN pripojenia"

2.4.4 Alternatíva M-D – "Poskytnutie nakonfigurovaného komunikačno-autentifikačného modulu zdravotníckym pracovníkom"
2.4.5 Multikriteriálna analýza
2.5 Výber alternatívy
2.6 Popis budúceho stavu
2.6.1 Legislatíva
2.6.2 Architektúra
2.6.3 Prevádzka
2.6.4 Ekonomická analýza

Zoznam obrázkov
No table of figures entries found.
Zoznam tabuliek
Tabuľka 1 Základné informácie - zhrnutie
Tabuľka 2 Skratky a značky
Tabuľka 3 Motivácia – budúci stav
Tabuľka 5 Biznis architektúra - aktuálny stav
Tabuľka 6 Architektúra informačných systémov - aktuálny stav
Tabuľka 7 Technologická architektúra - aktuálny stav
Tabuľka 8 Bezpečnostná architektúra - aktuálny stav
Tabuľka 9 Prevádzka - aktuálny stav
Tabuľka 17 Multikriteriálna analýza
Tabuľka 17 Multikriteriálna analýza
Tabuľka 10 Legislatíva - budúci stav
Tabuľka 11 Biznis architektúra – budúci stav
Tabuľka 12 Architektúra informačných systémov - budúci stav
Tabuľka 13 Technologická architektúra - budúci stav
Tabuľka 14 Implementácia a migrácia
Tabuľka 15 Bezpečnostná architektúra - budúci stav
Tabuľka 16 Prevádzka - budúci stav
Tabuľka 17 Ekonomická analýza - budúci stav

Základné informácie

Prehľad

Štúdiu uskutočniteľnosti národného projektu „Zabezpečenie efektívneho používania služieb ESO1 poskytovateľmi zdravotnej starostlivosti na celom území SR (projekt ESO1 – D)" vypracovala spoločnosť Ernst & Young, s. r. o. pre Národné centrum zdravotníckych informácií (ďalej len „NCZI"), ktoré je v zriaďovateľskej pôsobnosti Ministerstva zdravotníctva Slovenskej

republiky (ďalej len „MZSR"). Projekt Zabezpečenie efektívneho používania služieb ESO1 poskytovateľmi zdravotnej starostlivosti na celom území SR bude implementovať NCZI, ktoré bude aj žiadateľom o nenavratný finančný príspevok na jeho realizáciu.

Výsledkom projektu bude:

1. alternatívny mobilný spôsob autentifikácie a autorizácie zdravotníckeho pracovníka (ďalej aj "ZPr") v Systéme eZdravie a
2. implementácia Komunikačno-autentifikačného modulu (ďalej len "Komunikačno autentifikačný modul", alebo KAM skladajúci sa z "softvérovej časti - "KAM-sw" a hardvérová časť - "Inštancia KAM").

Výsledkom projektu bude pre alternatívu mobilnej autentifikácie a autorizácie aj nové serverové riešenie "Centrálny cryptocontroller" slúžiace na bezpečný prístup ZPr k záznamom eZdravie, ich podpisovanie a mobilná aplikácia pre autentifikáciu a autorizáciu prístupu do eZdravie v teréne alebo mimo PC ZPr. Rovnako výsledkom pre KAM bude presun všetkých centrálnych aplikačných komponentov eZdravie z počítača ZPr na KAM a nový softvér pre monitoring týchto komponentov ako aj nový softvér pre nahlasovanie chýb a incidentov na NCZI. Pre tých ambulantných PZS, ktorí nebudú požadovať Inštanciu KAM, bude poskytnutá len jeho softvérová časť KAM-sw, t.j. inštalácia centrálnych komponentov priamo na počítač ZPr vo vzdialenej správe NCZI.

Tabuľka 1 Základné informácie - zhrnutie

Zdôvodnenie využitia národného projektu a vylúčenia výberu projektu prostredníctvom výzvy	

Projekt je navrhnutý ako národný projekt. Celý projekt je v kompetenci NCZI, ako prevádzkovateľa Systému eZdravie, pričom kompetencie a zodpovednosť NCZI ustanovuje **zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme** a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Projekt je určený predovšetkým zainteresovaným stranám v rámci Systému eZdravie, a to najmä poskytovateľom zdravotnej starostlivosti, zdravotníckym pracovníkom (najmä lekári, sestry, záchranári) a pacientom, inštitúciám v rezorte zdravotníctva, ako aj všetkým občanom (široká verejnosť) bez ohľadu na ich trvalé bydlisko/sídlo.
Vláda Slovenskej republiky vo svojom programovom vyhlásení pre obdobie 2016 – 2020 v oblasti zdravotnej politiky určila ako jednu zo svojich priorít oblasť rozvoja, obnovy a modernizácie, tj. aj nové služby rezortu zdravotníctva pre jednotlivé subjekty sektora. Pre naplnenie týchto ambicióznych a náročných cieľov je potrebné reformovať oblasť poskytovania elektronických služieb rezortu tak, aby boli naplnené ciele a prínosy elektornického zdravotníctva na Slovensku. Táto štúdia uskutočnoteľnosti (ďalej aj "ŠU") bude súčasťou národného projektu.

Prijímateľa/partnera národného projektu a dôvod jeho určenia

Prijímateľom projektu je NCZI, ktoré je v zriaďovateľskej pôsobnosti MZSR. NCZI je subjekt zodpovedný za realizáciu informatizácie a elektronizácie zdravotníctva v Slovenskej republike.
Partnerom národného projektu bude Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (ďalej len „ÚPPVII"), ktorý je v zmysle ods. § 34a, bodu 1b) Zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov ústredným orgánom štátnej správy pre oblasť informatizácie spoločnosti. V súlade s Operačným programom Integrovaná infraštruktúra 2014 - 2020 si bude ÚPPVII uplatňovať maximálne 3 % oprávnených výdavkov projektu pre implementáciu štandardov riadenia informačno-technologických projektov, ktoré zabezpečia aktívnu participáciu na riadení projektu a komplexné riadenie budovania informačnej spoločnosti.

Príslušnosť národného projektu k relevantnej časti PO7 OPII	PRIORITNÁ OS Operačného programu integrovaná infraštruktúra PO7: Informačná spoločnosť TEMATICKÝ CIEĽ TC 2: Zlepšenie prístupu k IKT a zlepšenie ich využívania a kvality Investičná priorita 2c: Posilnenie aplikácií IKT v rámci elektronickej štátnej správy, elektronického vzdelávania, elektronickej inklúzie, elektronickej kultúry a elektronického zdravotníctva
Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu	13 406 439 Eur s DPH

Dôvod

Od 1. januára 2017 je v ostrej prevádzke Systém elektronického zdravotníctva, známy ako Systém eZdravie. Do Systému eZdravie sa ZPr prihlasujú cez svoje informačné systémy poskytovateľov zdravotnej starostlivosti (ďalej aj "IS PZS") a pristupujú doň výhradne prostredníctvom elektronického preukazu zdravotnického pracovníka (ďalej aj "ePZP"), ktorý majú počas práce s eZdravie stále vložený v čítačke ePZP. Z tohto dôvodu nie je v súčasnoti umožnený prístup takým zdravotníckych pracovníkom, ktorí pracujú a zapisujú zdravotné záznamy pacientov v teréne alebo mimo svojho PC. Typickým príkladom sú zdravotnícki záchranári, ZPr pracujúci pre Agentúru domácej ošetrovateľskej starostlivosti (tzv. "ADOS") alebo lekári v nemocnici na vizite pacienta. Absencia alternatívneho riešenia pre týchto ZPr má za následok fakt, že v súčasnosti pristupujú do eZdravie len čiastočne (lekár v nemocnici zapisuje a číta záznamy len z prostredia jeho ambulancie) alebo nepristupujú vôbec (ADOS setry alebo zdravotnícki záchranári priamo zo sanitky). Dôvodom vzniku prvej časti tejto ŠU je zanalyzovať najvhodnejšiu alternatívu mobilného prístupu týmto ZPr tak, aby súčasný stav prístup cez ePZP bol pre ostatných ZPr ponechaný. Mobilný prístup je nevyhnutnou prerekvizitou pre pripravovaný Národný projekt "Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (NZIS)", v rámci ktorého sa predpokladá integrácia systému záchrannej zdravotnej služby.

Ďaľšou a zároveň druhou príležitosťou na zlepšenie, z ktorej táto ŠU vychádza, je nutnosť odbremeniť ZPr od riešenia technických problémov eZdravie (nemyslia sa tým problémy súvisiace s inými systémami ako napr. jeho ambulantný systém) a ak aj keď takýto problém nastane, je potrebné zabezpečiť, aby mal čo najmenší dopad na samotného ZPr a nebol pre neho zdržaním alebo inou prekážkou v práci s eZdravie. Za súčasného riešenia je pre NCZI problematické v čo najkratšej dobe vyriešiť technický problém, pretože nevie monitorovať počítač ZPr a ani jeho IS PZS. Rovnako nevie monitorovať centrálne aplikačné komponenty

eZdravie, pretože sú inštalované buď na počítači ZPr alebo sú integrálnou súčasťou IS PZS. Dôvodom vzniku druhej časti ŠU je zanalyzovať najvhodnejší spôsob monitorovania aktivity lekára a vzdialeného prístupu k centrálnym aplikačným komponentov mimo počítač lekára a IS PZS tak, aby boli v plnej správe NCZI a bola zabezpečená kontinuálna práca ZPr v eZdravie a znížený odchod ZPr zo systému na minimum. Zabezpečenie kontinuity a eliminácia odchodu ZPr z eZdravie zároveň predstavuje v čo najväčšej miere naplnenie prínosov elektronického zdravotníctva na Slovensku. Zabezpečenie prevádzkyschopného riešenia je nevyhnutnou prerekvizitou (rovnako ako mobilný prístup do eZdravie) pre pripravovaný národný projekt "Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (NZIS)", ktorý predpokladá rozšírenie eZdravie o nové služby, čo nie je možné v prípade, ak súčasné služby nie sú plnohodnotne využívané zo strany ZPr.

Cieľmi ŠU je implementácia v nasledovných oblastiach:

1. alternatívneho mobilného prístupu (identifikácie, autentizácie a autorizácie) zdravotníckeho pracovníka:
    1. poskytnúť prístup do eZdravie mobilným ZPr, ktorí pracujú v teréne alebo mimo PC,
    2. poskytnúť v prípade požiadavky alternatívu ostatným ZPr, pričom hlavným spôsobom autentifikácie ostáva ePZP,
2. poskytnutia komunikačno autentifikačného modulu v správe NCZI, pričom sa:
    1. presunú centrálne aplikačné komponenty eZdravie (ovládače, klienti a cryptocontroller) mimo počítača ZPr do KAM a všetky komponenty bude NCZI môcť vzdialene spravovať,
    2. implementuje sa monitoring KAM a aplikačných komponentov a v prípade incidentu sa v čo najkratšej dobe vzdialene aktualizujú.

1.Alternatívny mobilný prístup (identifikácia, autentizácia a autorizácia) zdravotníckeho pracovníka

Prvým cieľom štúdie je umožniť zdravotníckym pracovníkom dodatkovú/alternatívnu formu prístupu do Systému eZdravie, nakoľko zdravotnícky pracovník potrebuje pracovať so systémom eZdravie aj mimo svojej koncovej stanice (napr. vizita, záchranná zdravotná služba, práca v teréne (ADOS) a iné). Pre tieto prípady je potrebné zabezpečiť mobilnú alternatívu autentifikácie a autorizácie zdravotníckeho pracovníka. Mobilná autentifikácia rovnako odbúra procesné úkony súvisiace so stratou, odcudzením alebo nutnosťou prevydania elektronického preukazu zdravotníckeho pracovníka alebo PIN kódu. Zo štatistík NCZI vyplynulo, že je relevantná pre ZPr v počte 31 990 nasledovne:

Druhy zdravotníckych zariadení		Počet			
		pracovných miest lekárov	pracovných miest zubných lekárov	pracovných miest sestier	pracovné miesta záchranárov
SPOLU CELKOVO					**31 990**
SPOLU		**9 441**	**86**	**20 598**	**1 864**
Ambulantná zdravotná starostlivosť		**437**	**13**	**836**	**1 864**
v tom	ambulancia záchrannej zdravotnej služby	230	0	24	1 864
	agentúra domácej ošetrovateľskej starostlivosti	0	0	604	-
	mobilný hospic	4	0	5	-
	ambulancia lekárskej služby prvej pomoci	204	13	202	-
Ústavná zdravotná starostlivosť vrátane ambulantných častí		**8 999**	**73**	**19 739**	
v tom	všeobecná nemocnica	7 840	69	16 891	-
	špecializovaná nemocnica	1 160	3	2 848	-
Ostatné		**5**	**0**	**24**	
v tom	dopravná zdravotná služba	0	0	20	-
	mobilné zariadenie PZS, na základe licencie na výkon samostatnej zdravotníckej praxe	5	0	4	-

Z celkového počtu ZPr, pre ktorých je mobilný prístup relevantný, je celkovo 2 118 ZPr ambulancie záchrannej zdravotnej služby, ktorí bez mobilnej autentifikácie nevedia pracovať v eZdravie, pretože pracujú výhradne v teréne:

Druhy zdravotníckych zariadení		Počet			
		pracovných miest lekárov	pracovných miest zubných lekárov	pracovných miest sestier	pracovné miesta záchranárov
SPOLU CELKOVO					**2 760**
SPOLU		**239**	**0**	**657**	**1 864**
Ambulantná zdravotná starostlivosť		**234**	**0**	**633**	**1 864**
v tom	ambulancia záchrannej zdravotnej služby	230	0	24	1 864
	agentúra domácej ošetrovateľskej starostlivosti	0	0	604	-
	mobilný hospic	4	0	5	-
Ostatné		**5**	**0**	**24**	
v tom	dopravná zdravotná služba	0	0	20	-
	mobilné zariadenie PZS, na základe licencie na výkon samostatnej zdravotníckej praxe	5	0	4	-

Hlavnou úlohou elektronického preukazu zdravotníckeho pracovníka (ďalej ako „ePZP") je identifikácia, autentizácia a autorizácia zdravotníckeho pracovníka. ePZP obsahuje tiež aj tzv. súkromné kľúče a certifikáty, ktoré slúžia na účely vytvárania elektronického podpisu zdravotníckeho pracovníka a šifrovanie/dešifrovanie údajov. Tieto vlastnosti je potrebné v čo najväčšej miere zachovať, avšak súčasne zlepšiť použiteľnosť riešenia tak, aby na prístup k systému bolo možné využiť aj inú autentifikáciu ako ePZP.

Zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov ustanovuje v súvislosti s elektronickým preukazom zdravotníckeho pracovníka určité povinnosti:

1. povinnosť chrániť elektronický preukaz pred zničením, poškodením, stratou, odcudzením a zneužitím,
2. ak by došlo k vyššie uvedeným udalostiam, zdravotnícky pracovník musí bezodkladne oznámiť NCZI takúto stratu, odcudzenie alebo zničenie elektronického preukazu,
3. povinnosť uviesť v žiadosti o vydanie elektronického preukazu úplné a pravdivé údaje a ich správnosť potvrdiť svojím podpisom. Ide o údaje ako meno a priezvisko, zdravotnícke povolanie, ktoré vykonáva, jeho registračné číslo, označenie stavovskej organizácie, v ktorej je registrovaný (lekárska komora, komora sestier a pôrodných asistentiek a pod.).

2.Komunikačno autentifikačný modul (KAM)

Druhým cieľom štúdie je zabezpečiť kontinuálnu a bezproblémovú prácu zdravotníckeho pracovníka v Systéme eZdravie. Problém rýchleho riešenia chýb je v súčasnosti evidovaný na strane ambulantných poskytovateľov, ktorí na rozdiel od nemocníc nemajú vlastné IT oddelenie a IT problémy riešia buď sami alebo s pomocou svojho dodávateľa IS PZS. Rozsah problému je ilustrovaný v nasledovnom rozdelení, jedná sa celkovo o 11 442 ambulancií:

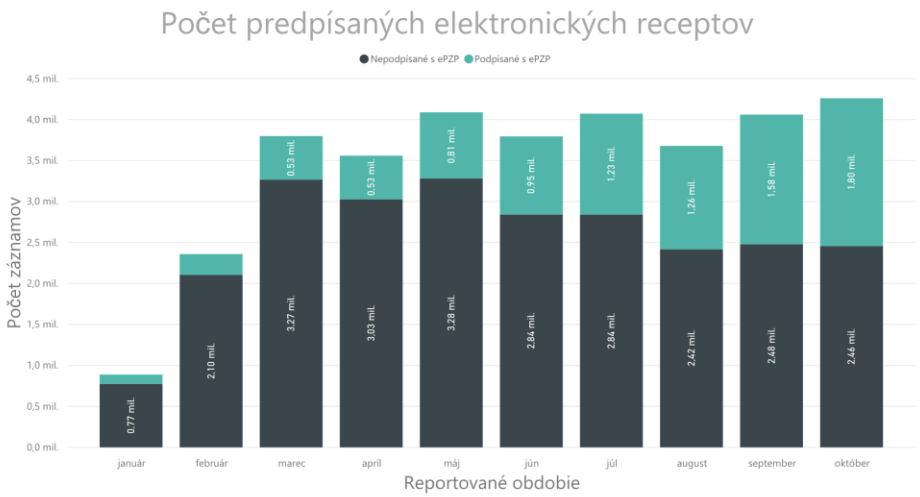
	Celkový počet	ambulancia	pracovisko	stacionár	útvar jednodňovej zdravotnej starostlivosti	útvar spoločných vyšetrovacích a liečebných zložiek
ambulancia všeobecnej ambulantnej zdravotnej starostlivosti	**2 709**	2 709				
ambulancia špecializovanej ambulantnej zdravotnej starostlivosti	**6 867**	6 817	17			33
zariadenie na poskytovanie jednodňovej zdravotnej starostlivosti	**227**	102			125	
stacionár	**175**	88	5	81		1
poliklinika	**779**	643	5	13	36	82
zariadenie spoločných vyšetrovacích a liečebných zložiek	**557**					557
ambulancia lekárskej služby prvej pomoci	**128**	128				
Spolu	**11 442**	10 487	27	94	161	673

V prípade, ak nastane chyba, zdravotnícky pracovník má možnosť jej nahlásenia len prostredníctvom call centra NCZI, kde slovne popíše problém (na základe štatistík Call centra NCZI bolo identifikované priemerné trvanie hovoru 3 minúty) a nemá možnosť/nevie zaslať štruktúrovaný záznam udalosti pre rýchlejšie vyriešenie chyby. Vo väčšine prípadov sa stáva, že NCZI musí opätovne volať ZPr pre dodatočné informácie, v krajnom prípade musí uskutočniť výjazd k ZPr. Vzhľadom na kritickosť systému a nehomogénosť celého prostredia (viac ako 70 dodávateľov informačných systémov poskytovateľov zdravotnej starostlivosti), NCZI dokáže monitorovať len centrálny Systém eZdravie bez možnosti analýzy problému E2E, tj. od

centrálnych aplikačných komponentov eZdravie inštalovaných na počítači ZPr až po centrálny Systém eZdravie.

Je potrebné podotknúť, že IS PZS je hrubý klient inštalovaný na počítači ZPr a jeho integrálnou súčasťou je aj centrálny aplikačný komponent Cryptocontroller, ktorý vydáva NCZI. Kedže sa jedná o hrubého klienta IS PZS, NCZI nedokáže k Cryptocontrolleru pristupovať vzdialene, tz., že v prípade vydania aktualizácie Cryptocontrollera, musí vydať integračný manuál s popisom aktualizácie a osloviť každého jedného dodávateľa s požiadavkou na úpravu IS PZS. V zmysle zákona a pravidiel overenia zhody IS PZS, má dodávateľ 60 dní na zapracovanie zmeny IS PZS. Pri súčasnom nastavení teda nie je veľmi obtiažne v réžii NCZI riadiť opravy chýb a aktualizácie centrálnych aplikačných komponentov. Predlžuje sa čas zdravotníckeho pracovníka na nahlásenie problému a čas potrebný na dodatočné dohľadávanie informácií a riešenie problému, čo znižuje motiváciu používania systému už zapojených zdravotníckych pracovníkov, v hraničných prípadoch spôsobuje nepoužívanie Systému eZdravie. V ambulatnom sektore je ešte stále využívaná nepodporovaná a zastaralá verzia OS Windows XP (37 percent), čo môže spôsobiť postupné znemožnenie pripojenia do eZdravie - niektoré aplikačné komponenty eZdravie nepodporujú alebo v blízkej dobe nebudú podporovať Windows XP. Z toho dôvodu je potrebné zabezpečiť proaktívny monitoring a vzdialené aktualizácie centrálnych komponentov, ktoré sú v súčasnosti inštalované na počítačoch ZPr alebo v rámci IS PZS. Centrálna správa aplikačných komponentov a E2E monitoring KAM značne odbúra čas potrebný na nahlásenie problému v rámci eZdravie, priebežné sledovanie KAM zabezpečí predikciu potenciálneho problému a rovnako vzdialená správa zabezpečí rýchle nasadenie opravy chýb a aktualizáciu centrálnych aplikačných komponentov. Jedným z reprezentatívnych príkladov je globálna aktualizácia systému Windows 10, ktorá v období Január-Marec 2018 spôsobil problém, kedy ZPr pri každom systémovom úkone s eZdravie musel opätovne zadávať PIN (cca každých 5s). NCZI nevedelo ovplyvniť eliminovať tento problém, pretože väčšina ZPr malo nastavenú automatickú inštaláciu Windows. Uvedený problém spôsobil, že zdravotnícki pracovníci prestali načas pracovať v systéme (pokles o 6,3%ZPr) a dokonca, aj po vyriešení chyby, už následne systém eZdravie nepoužívali (4,3%). V rámci analýzy budúceho stavu robilo NCZI prieskum u ambulantných lekárov, ktorí podporili alternatívu inštancie KAM a zámer tohto riešenia. Ako jednu z výhod riešenia uviedli úsporu času venovanému nahlasovaniu incidentov, riešenie incidentov na strane ZPr a zníženie času pre nasadenie nových verzií.

Rovnako dôležité je spomenúť, že pre správny chod ePZP karty a jej používanie, je dôležité mať správne nainštalovanú aktuálnu verziu Cryptocontrollera, teda jeden z aplikačných komponentov eZdravie. V súčasnosti len 43% ZPr predpisuje recepty a podpisuje ich ePZP kartou. Zvyšných 57% musí recepty tlačiť. Na to, aby bola dosiahnutá 100% používanosť ePZP, musí byť Cryptocontroller v plnej správe NCZI, ktoré ho bude môcť aktívne riadiť, monitorovať a aktualizovať. Nasledujúci obrázok ilustruje vývoj používania ePZP.



Táto štúdia definuje príležitosti na zlepšenie v nasledovných oblastiach:

- zabezpečenie alternatívnej autentifikácie zdravotníckych pracovníkov do systému eZdravie,

- zabezpečenie KAM pre ambulantný sektor s potrebnou funkcionalitou, schopnosťou centrálne udržiavať aplikačné komponenty na koncovej stanici zdravotníckeho pracovníka a potrebnou úrovňou bezpečnosti,
- zabezpečenie systému monitoringu a bugreportingu prostredníctvom KAM a jeho implementácia.

Implementáciou navrhovaných opatrení dôjde k nasledovným zlepšeniam:

- sprístupnenie eZdravie pre záchranárov v počte 2 118,
- odstránenie prestojov pre 50% (hodnota vyplýva zo zvolenej nábehovej krivky) ZPr pri strate alebo odcudzení ePZP (2 dni),
- odstránenie prestojov pre 50% (hodnota vyplýva zo zvolenej nábehovej krivky) ZPr pri strate alebo zabudnutí PIN (2 dni),
- zníženie nákladov na správu a prevydávanie ePZP pre 50% ZPr,
- zrýchlenie používania eZdravia vďaka rýchlejšej autentifikácii ako aj rýchlejšiemu odstraňovaniu menšieho množstva incidentov,
- zníženiu odpájania používateľov eZdravia, na základe negatívnych skúseností (napr. nemožnosť sa prihlásiť),
- zvýšenie prínosov eZdravia vďaka bezproblémovej práce zdravotníckeho pracovníka,
- odstránenie prestojov pri práci zdravotníckeho pracovníka vďaka centrálnej správe aplikačných komponentov eZdravie,
- zníženie času zdravotníckeho pracovníka potrebného na nahlasovanie incidentov,
- zníženie času na dohľadávanie informácii a riešenie problému na strane NCZI,
- zníženie počtu incidentov vďaka predikcii chýb a incidentov,
- zrýchlenie zápisu zdravotných záznamov vďaka monitoringu E2E procesu zápisu záznamu,

- zníženie nákladov na odstraňovanie incidentov,
- zlepšeniu image eZdravia u používateľov.

Projekt rieši aktuálny stav využívania eZdravia (pričom nerealizovaním projektu je predpoklad, že tento stav bude pretrvávať):

- zdravotnícki pracovníci pracujúci v teréne minimálne v počte 2 118 (záchranári) nebudú môcť využívať eZdravie, čo činí zníženie prínosov eZdravie o 4 768 577 Eur,
- v prípade praktických problémov s ePZP, ako je strata alebo zničenie karty dochádza k značnému prestoju na strane lekára spôsobeného procesom výroby novej ePZP, čo predstavuje 2 dni,
- nepravidelná/prerušovaná práca v eZdravie – prestoje zaznamenané v prípade nutnosti nasadenia aktualizácie centrálnych aplikačných komponentov. Nasadenie aktualizácií je zdĺhavé vzhľadom na to, že úprava centrálneho komponentu vyžaduje aj úpravu IS PZS. To spôsobuje, že zdravotnícki pracovníci eZdravie prestanú na určitý čas používať alebo sa k používaniu eZdravie nevrátia aj po vyriešení problému,čo predstavuje zníženie prínosov 3 652 541 Eur ročne,
- nákladovosť súčasného riešenia incidentov na strane ZPr a NCZI, čo predstavuje náklady na jednu úpravu (u každého dodávateľa IS PZS) v sume 4 000 Eur, ktoré znáša samotný ZPr,
- systém eZdravie nemá pozitívny obraz medzi odbornou verejnosťou, jednak vďaka zložitej inštalácii aplikačných komponentov ako aj incidentom, z ktorých veľa je spôsobených problémom na koncovej stanici ZPr.

Rozsah

ŠU vychádza z metodického usmernenia pre spracovanie štúdií uskutočniteľností v rámci Operačného programu Integrovaná infraštruktúra, Prioritná os 7, špecificky pre štúdie zamerané na cloudové služby. Venuje sa posúdeniu súčasného stavu eZdravia, identifikuje problémové oblasti, posudzuje alternatívne riešenia, ktorými je možné zlepšiť súčasný stav a navrhuje cieľový stav – vybudovanie riešenia eZdravia v plnom rozsahu, ale najmä so zameraním na alternatívnu autentifikáciu, identifikáciu zdravotníckeho pracovníka a monitoring koncových zariadení ZPr.

Navrhované riešenia štúdie reflektujú požiadavky NCZI, ktorých cieľom je najmä zabezpečiť prevádzkyschopné riešenie a poskytnúť ZPr bezproblémovú prácu v eZdravie. Štúdia popisuje súčasný stav identifikácie, autentizácie a autorizácie ZPr v Systéme eZdravie a spôsob riešenia a monitorovania prevádzky Systému eZdravie, navrhuje budúci stav riešenia mobilnej identifikácie, autentizácie a autorizácie ZPr a riešenie správy centrálnych komponentov prostredníctvom KAM.

Navrhované riešenia ponímajú problém a príležitosti na zlepšenie pre oba ciele štúdie komplexne. Vytvára tak priestor pre prístup všetkých ZPr do eZdravie a poskytuje spôsob ako zabezpečiť bezproblémovú prevádzku centrálneho systému a jeho komponentov bez zbytočného časového alebo finančného zaťaženia ZPr.

Ohraničenie situácie je možné vyjadriť nasledovnou tabuľkou:

Oblasť	Aktér	Rola	ISVS
Mobilný prístup ZPr	Podnikateľ	Zdravotnícky pracovník (lekár, sestra, farmaceut, sanitár, lekárnik, masér, atď, cca 110 000 ZPr, ktorým má byť vydaná ePZP), ktorý sa pri prístupe do systému autentifikuje kartou ePZP. Mobilní prístup je pre nich alternatívou k ePZP.	eZdravie - isvs_400
	Podnikateľ	Zdravotnícky pracovník (záchranár, ADOS pracovník, lekár na vizite a pod., cca 30 000 ZPr) ktorí potrebujú pristupovať do eZdravie mimo svojho PC, tj. bez ePZP prostredníctvom mobilného zariadenia (tabletu). Mobilný prístup by im mal byť umožnený.	eZdravie - isvs_400
	Podnikateľ	Zdravotnícky pracovník (záchranár, cca 1 864), ktorí nevyhnutne potrebujú pristupovať do eZdravie mimo svojho PC, tj. prostredníctvom mobilného zariadenia (tabletu). Mobilný prístup je pre nich nevyhnutný.	eZdravie - isvs_400
Komunikačno autentifikačný modul (KAM)	Podnikateľ	Zdravotnícky pracovník v rámci ambulantného sektora mimo nemocníc (lekár + sestra v cca 11 442 ambulanciách), ktorý rieši problémy s používaním eZdravia, napríklad: • inštalácia nových ovládačov pre používanie ePZP na svojom počítači, • nahlasovanie problémov a chýb, • nefunkčnosť systému (spôsobená problémom na strane lekára alebo NCZI).	eZdravie - isvs_400
	NCZI	Správca ePZP, ktorý rieši životný cyklus ePZP. Správca centrálnych komponentov potrebných pre fungovanie IS PZS.	eZdravie - isvs_400
	NCZI	Správca systému eZdravie, ktorý rieši incidenty spojené so systémom.	eZdravie - isvs_400
	MZ SR	Dohľad nad systémom eZdravie, subjekt, ktorého záujmom je čo najväčie rozšírenie používania eZdravia medzi zdravotníckymi pracovníkmi.	eZdravie - isvs_400
	Občan	Pacient, ktorý chce čo najrýchlejšie ošetrenie a zároveň má záujem o zníženie papierovej byrokracie.	eZdravie - isvs_400

Štúdia pokrýva popis súčasného stavu a popis budúceho stavu pre 2 oblasti štúdie:

1. **Alternatívny mobilný prístup (identifikácia, autentizácia a autorizácia) zdravotníckeho pracovníka a**
2. **Komunikačno autentifikačný modul (KAM)**

z pohľadu:

- legislatívy, do ktorého budú obe oblasti implementované, jedná sa najmä o úpravu súčasne platných zákonov a vyhlášok,
- biznis riešenia kľúčových procesov, ktoré navrhované riešenia optimalizuje najmä z pohľadu času,
- architektúry riešenia, v ktorom budúce riešenie je navrhnuté tak, aby bolo v súlade so súčasným riešením a aby nové prvky architektúry neohrozili koncepciu súčasného riešenia a boli v súlade so stratégiou riešenia do budúcnosti,
- architektúry centrálneho riešenia mobilnej autentifikácie a autorizácie a KAM, ktorá znázorňuje najmä integráciu z pohľadu IS PZS,
- bezpečnostnej architektúry tak, aby nebola ohrozená alebo znížená úroveň bezpečnosti súčasného riešenia,
- motivácie, ktorá vychádza z požiadaviek NCZI a poskytovateľov zdravotnej starostlivosti,
- nasadenia a prevádzky budúceho riešenia, ktoré využíva súčasné kapacity NCZI,
- nákladov a prínosov, kde ekonomická analýza kvantifikuje a popisuje náklady a prínosy vyplývajúce z implementácie oboch oblastí riešenia.

Pre obe oblasti štúdie menované vyššie sú definované ciele a biznisové kritéria, ktoré je potrebné naplniť a ktoré sú samotnými požiadavkami na výber najvhodnejšej alternatívy. Štúdia však najprv analyzuje možné technické riešenia a z nich sú koncipované biznis alternatívy.

Použité skratky a značky

Tabuľka 2 Skratky a značky

Skratka / Značka	**Vysvetlenie**
AD	Adresárové služby Active directory
ADFS	Federačné služby AD
ADOS	Agentúra domácej ošetrovateľskej starostlivosti
API	Funkcie pre prístup k aplikácii cez internet
eIDAS	Nariadenie európskeho parlamentu o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu
ePZP	Elektronický preukaz zdravotníckeho pracovníka
ESO1	Projekt Elektronické služby zdravotníctva

ESZ	Elektronické služby zdravotníctva
EÚ	Európska Únia
IKT	Informačné a komunikačné technológie
IS PZS	Informačný systém poskytovateľa zdravotnej starostlivosti (ambulantný, nemocničný alebo lekárenský softvér)
IT	Informačné technológie
JRÚZ	Jednotná referenčná údajová základňa
KZ	Koncové zariadenie
KPI	Key performance indicator (Kľúčový ukazovateľ výkonnosti)
MitM	Útok typu Man in the middle
MZSR	Ministerstvo zdravotníctva SR
NCZI	Národné centrum zdravotníckych informácií
NZIS	Národný zdravotnícky informačný systém
OPII	Operačný program integrovaná infraštruktúra
OPIS	Operačný program informatizácia spoločnosti
PO7	Prioritná os 7
PZS	Poskytovateľ zdravotnej starostlivosti
RFaRS	Rozšírenie funkcionality a rozsahu služieb
SQL	Databázový jazyk
STS	Poskytovanie bezpečnostných tokenov za účelom autentifikácie
SW	Softvér
ŠU	Štúdia uskutočniteľnosti
TPM	Trusted platform module
ÚPVS	Ústredný portál verejnej správy
ÚPPVII	Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu
VS	Verejná správa
KAM	Komunikačno autentifikačný modul
SW	Softvér
ZPr	Zdravotnícky pracovník

Manažérske zhrnutie

Systém eZdravie prevádzkuje Národné centrum zdravotníckych informácií, pričom na základe skúseností z prevádzky eviduje nasledovné problematické oblasti:

1. Systém neumožňuje prístup mimo ambulancie lekára, tj. napr. záchranársky pracovník alebo ADOS pracovník sa nevedia z terénu prihlásiť do eZdravie
2. Centrálne komponenty eZdravie sú súčasťou PC lekára alebo sú integrálnou súčasťou IS PZS, na ktoré NCZI nemá dosah a tak nemá možnosť monitorovať, riadiť životný cyklus

týchto komponentov, ich aktualizácie a opravy, čo vedie k zdĺhavému riešeniu problémov a incidentov, pretože každá aktualizácia si vyžaduje úpravu samotného IS PZS. Zdĺhavé riešenie má za následok prerušovanú prácu ZPr v systéme, až samotný odchod ZPr zo systému.

Nevyhnutnými krokmi pre elimináciu vyššie popísaných problematických oblastí a rovnako ciele pre zabezpečenie plnohodnotnej prevádzky eZdravie sú:

1. Umožnenie prístupu do eZdravie pre zdravotníckych pracovníkov pracujúcich v teréne (napr. záchranári, ADOS pracovníci) alebo mimo ambulancie (lekári na vizite) a
2. Centrálne riadenie aplikačných komponentov eZdravie na úrovni NCZI, ktoré budú vysunuté v module pre autentifikáciu a komunikáciu (KAM) určené pre ambulantný sektor v podobe inštancie KAM, pre IT zdatnejších ZPr ponúkne NCZI tzv. KAM-sw, tj. softvérovú verziu, ktorú si ZPr sám nainštaluje na svoje PC.

Najvýznamnejšími KPI projektu sú:

- počet dodatočných elektronických služieb pre poskytovateľov, ktoré je možné riešiť mobilným zariadením: 1(sluzba_is_33215),
- počet ZPr pracujúcich v teréne, ktorí vedia mobilne pristupovať do eZdravie: 1 864,
- zavedenie mobilnej autentifikácie s penetráciou 50% ZPr,
- zvýšenie využívania ePZP pri podpisovaní predpísaných elektronických receptov na 100%, aktuálne 43% (v prípade využitia KAM),
- zníženie počtu komponentov a driverov inštalovaných samotným lekárom pre pripojenie IS PZS do eZdravia na 0 (v prípade využitia KAM),
- zvýšenie dostupnosti vidieť stav centrálnych komponentov: na 100% (v prípade využitia KAM inštancie),
- zníženie času potrebného pre nahlásenie incidentu: o 73% (v prípade využitia KAM inštancie),

1. **Alternatívny mobilný prístup (identifikácia, autentizácia a autorizácia) zdravotníckeho pracovníka**

Pre naplnenie prvého cieľu je nevyhnutné poskytnúť zdravotníckemu pracovníkovi možnosť identifikácie a autentifikácie zdravotníckeho pracovníka bez ePZP karty vloženej v ePZP čítačke. Na základe multikriteriálnej analýzy bolo odporučené riešenie, ktoré presúva funkcionalitu cryptocontrollera z pracovných staníc zdravotníckych pracovníkov do serverovej časti, čím umožní nový spôsob autentifikácie prostredníctvom mobilného zariadenia, avšak naďalej hlavným spôsobom prístupu ostáva ePZP karta. Z pohľadu používateľov nie sú zmeny zásadné, výhodou je, že karta ePZP nebude musieť byť vložená v čítačke celý čas a pribudne možnosť prihlásenia sa do systému eZdravie aj cez mobilné zariadenie. Rovnako štúdia predpokladá, že vzhľadom na vývoj mobilných služieb, prístup do eZdravie prostredníctvom mobilného zariadenia budú využívať aj takí ZPr, ktorí nepracujú v teréne. Riešenie prináša zvýšenie prínosu

z eZdravie pre tých ZPr, ktorí v súčasnoti nemajú prístup do eZdravie a samotné zníženie nákladov spojených s prevádzkou a vydávaním ePZP.

Navrhované riešenie prinesie pre ZPr najmä alternatívnu možnosť prístupu do eZdravie, umožní prístup najmä pre ZPr pracujúcich v teréne (ako záchranári, ADOS pracovníci, lekári na vizitách v nemocniciach). V prípade, ak by toto riešenie nebolo implementované, ZPr by mali prístup k eZdravie len cez PC a pre záchranárov alebo ADOS sestry by bol takýto prístup ťažko využiteľný, keďže väčšina ich práce a vytvárania zdravotných záznamov sa vykonáva mimo PC.

Prínosy pre mobilný prístup ZPr (identifikácia, autentifikácia a autorizácia) sú nasledovné:

- riešenie do budúcnosti podporuje aj mobilné eZdravie (t.j. multikanálový prístup k službám)
- zjednodušuje nasadenie na koncové zariadenie lekára (ak lekár nepoužíva autentifikáciu pomocou karty, nie je potrebné na koncové zariadenie inštalovať žiadne ďalšie komponenty alebo ovládače, nie je potrebné riešiť životný cyklus karty a jej distribúciu v prípade jej straty alebo odcudzenia, riešiť zasielanie nového PIN v prípade jeho zabudnutia)
- riešenie umožní dynamickejšie pridávať nové role, resp. používateľov systému (nebude potrebné distribuovať fyzické karty),
- riešenie umožní lekárom výber autentifikácie, ktorá im vyhovuje (ePZP karta alebo alternatívny spôsob bez ePZP karty) ,
- po úvodnej registrácii nevyžaduje už žiadny ďalší token, čip, čítačka, kábel ani iné zariadenie – iba spárované mobilné zariadenie, prostredníctvom ktorého sa zdravotný pracovník bude prihlasovať do systému,
- poskytuje aj možnosť prípadnej autorizácie prostredníctvom KEPu - najvyšší stupeň (podľa nariadenia eIDAS).

Náklady pre mobilný prístup ZPr (identifikácia, autentifikácia a autorizácia) sú nasledovné:

- náklady na presun funkcionality cryptocontrollera do serverovej časti NZIS,
- náklady na vytvorenie mobilnej softvérovej aplikácie umožňujúcu identifikáciu a autentizáciu zdravotného pracovníka alternatívnym spôsobom bez použitia ePZP karty,
- náklady na softvérové riešenie a príslušné softvérové licencie poskytujúce funkcionalitu identifikácie a autentizácie zdravotného pracovníka prostredníctvom mobilného zariadenia,
- náklady na prevádzku SW a HW časti riešenia (podporované platformy),
- náklady na support, podporu a servis SW+HW časti riešenia (podporované platformy),
- vyvolané náklady dodávateľov IS PZS.

2. Komunikačno autentifikačný modul (KAM)

Pre naplnenie druhého cieľu ŠU navrhuje dodať pre jednotlivé ambulancie (mimo nemocničných) prípojné inštancie KAM a pre IT zdatnejších ZPr iba jeho softvérovú verziu (KAM-sw), ktorú si ZPr nainštaluje na svoje PC. Inštancia KAM má vlastný podporovaný operačný systém, obsahuje všetky potrebné periférne zariadenia pre prácu v eZdravie (čítačky

kariet ePZP a eID, čítačku kódov), obsahuje všetky centrálne aplikačné komponenty eZdravie, aplikáciu pre monitoring týchto komponentov a bugreporting. KAM-sw je balík centrálnych komponentov eZdravie a je taktiež v práve NCZI, na rozdiel od inštancie, si KAM-sw zdravotnícky pracovník inštaluje sám ako aj jeho aktualizácie (softvér však bude mať schopnosť automatickej aktualizácie). Aplikáciou tohto návrhu sa zabezpečí efektívnejšie nasadzovanie aktualizácií centrálnych aplikácií (driverov a cryptocontrollera), pre inštanciu KAM sa odbúra nutnosť inštalovať komponenty a drivery samotným ZPr, zaistí sa indepedencia inštancie so svojím vlastným profilom a jej odolnosť voči vplyvom globálnych aktualizácií, zaistí sa možnosť riešenia problémov zo strany NCZI a zabezpečí sa plnohodnotná a efektívna podpora ZPr zo strany NCZI. V prípade vzniku incidentu bude mať NCZI ucelený prehľad o stave centrálnych komponentov a samotného KAM. Nasadením centrálnych komponentov eZdravie do KAM sa odbúra nutnosť upravovať IS PZS zakaždým, keď výde nová verzia centrálneho komponentu, pretože tieto aplikácie už nebudú viac integrálnou súčasťou IS PZS. Riešenie prináša zníženie času na riešenie incidentu na strane lekára a NCZI, zvýšenie aktivity a zabezpečenie kontinuity práce v systéme eZdravie a zníženie odchodu už pripojených ZPr a celkové zlepšenie obrazu eZdravie u širokej a odbornej verejnosti.

Navrhované riešenie je určené pre ambulantných lekárov a sestry, ktorí nedisponujú vlastným IT oddelením a všetky technické problémy musia riešiť sami alebo pomocou dodávateľov IS PZS. Pre ambulantných lekárov a sestry prinesie toto riešenie najmä úsporu ich času, ktorý musia venovať riešeniu technických problémov a najmä úsporu ich financií, keďže každú úpravu IS PZS znáša poskytovateľ zdravotnej starostlivosti. Riešenie taktiež prinesie možnosť plnohodnotne prevádzkovať Systém eZdravie pre NCZI, ktoré bude mať plnú kontrolu nad centrálnymi komponentmi. Riešenie rovnako prinesie štátu zvýšené prínosy z eZdravie, keďže lekári budú v eZdravie kontinuálne pracovať a nebudú z neho odchádzať kvôli zdĺhavému riešeniu incidentov. V neposlednom rade riešenie prinesie aj zlepšenia pre samotného občana, ktorý nebude musieť kvôli nefunkčnosti eZdravie so sebou nosiť papierovú dokumentáciu alebo recepty.

Prínosy pre Komunikačno autentifikačný modul (KAM):

- dodáva lekárovi modul, resp. inštanciu, ktorý je plne v správe NCZI, čo umožní agilnejšie a komplexne riešiť prípadné incidenty,
- dodáva lekárovi modul, resp. inštanciu s preddefinovanými a preinštalovanými všetkými potrebnými komponentami, ktoré sú potrebné pre prístup do systému eZdravie a zároveň je plne v správe NCZI, čo umožňuje efektívnu vzdialenú aktualizáciu už nainštalovaných komponentov alebo vzdialenú inštaláciu opráv, fixov alebo nových komponentov,dodáva lekárovi rýchlejšie riešenie incidentov, čo šetrí čas a umožňuje efektívnejšie poskytovať zdravotnú starostlivosť,
- dodáva lekárovi informácie o stave Systému eZdravie.

Náklady pre Komunikačno autentifikačný modul (KAM):

- náklady na vybudovanie a support systému pre centrálny monitoring (klientská aj serverová časť),
- náklady na lokálnu bugreportingovú resp. monitorovaciu aplikáciu,

- náklady na hardvérovú inštanciu,
- náklady na softvérovú časť (SW),
- vyvolané náklady dodávateľov IS PZS.

Na základe kvantifikovaný nákladov a prínosov oboch riešení bola vypočítaná návratnosť projektu v 3 roku realizácie projektu.

Nevyhnutnou súčasťou sú externalizované požiadavky na zmenu u dodávateľov zdravotníckeho SW (IS PZS) – ktorí musia upraviť svoj SW plánovaným zmenám na úrovni cryptocontrollera. Nevyhnutnou súčasťou sú náklady súvisiace s hardvérom potrebným pre zabezpečenie oboch častí štúdie, náklady budú riešené v réžii NCZI.

Motivácia

Tabuľka 3 Motivácia – budúci stav

Súhrnný popis

Vláda Slovenskej republiky vo svojom programovom vyhlásení pre obdobie 2016 – 2020 v oblasti zdravotnej politiky určila ako jednu zo svojich priorít oblasť rozvoja, obnovy a modernizácie, to je aj nové služby rezortu zdravotníctva pre jednotlivé subjekty sektora.

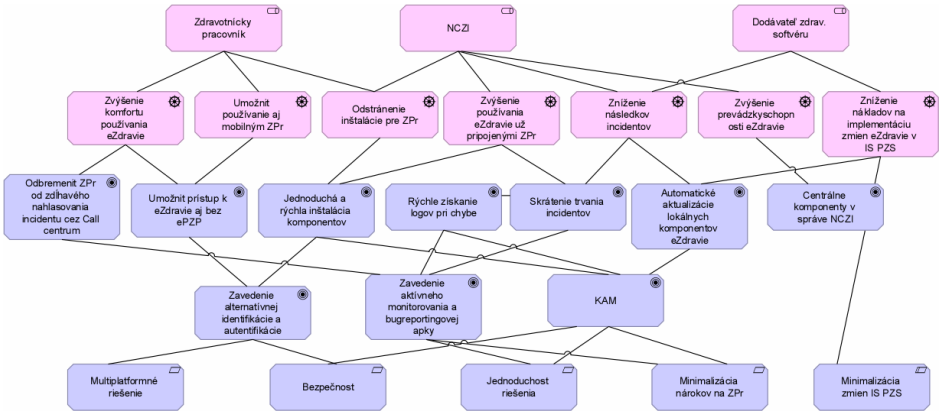
Táto ŠU prináša zavedenie alternatívnej identifikácie a autentifikácie zdravotníckeho pracovníka ako aj zavedenie systému monitorovania a reportovania incidentov spojených s využívaním systému eZdravie.

Predpokladajú sa najmä prínosy pre používateľov

- možnosť mobilného prístupu pre ZPr,
- odbremenenie ZPr od nahlasovania incidentov,
- odbremenenie ZPr od nutnosti inštalácie komponentov,
- zníženie nákladov na IS PZS,

ako aj prevádzkovateľa systému eZdravie vo forme:

- možnosť manažovať a predikovať možné problémy v budúcnosti,
- zvýšenie zabezpečenia ukladaných údajov na PC zdravotníckeho pracovníka,
- zefektívnenia riešenia incidentov,
- zníženia prevádzkových nákladov,
- zjednodušenia prevádzky,
- zrýchlenia troubleshootingu eZdravia.



Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Motivation viewpoint"

Aktér	Cieľ	Požiadavka	Obmedzenie
Zdravotnícky pracovník	Zvýšenie komfortu používania eZdravie	Je potrebné odbremeniť ZPr od zdĺhavého nahlasovania incidentu a zložitého dohľadávania logov. Je potrebné odstrániť technické problémy pri používaní eZdravie.	Je potrebné riešiť nielen problémy IS eZdravie, ale komplexne aj problémy na strane IS PZS, aby mal ZPr jedno rozhranie pre riešenie problémov
KPI	Čas potrebný na nahlásenie incidentu	Hodnota AS IS: 3 min Hodnota TO BE (2022):45 s	
Zdravotnícky pracovník	Umožnit používať eZdravie aj mobilným ZPr	Je potrebné umožniť prístup k eZdravie aj bez ePZP - pomocou inej formy autentifikácie	Pri implementácii je potrebné zachovať požadovanú úroveň bezpečnosti. Projekt realizuje iba zmenu identifikácie a autentifikácie, nevytvára ani nemení samotné koncové služby.
KPI	Penetrácia používania mobilného ePZP Počet dodatočných elektronických služieb pre podnikateľov, ktoré je možné riešiť mobilným zariadením.	Hodnota AS IS: 0 Hodnota TO BE (2022):50% Hodnota AS IS: 0 Hodnota TO BE (2022):1 (cez mobilné ePZP)	

Zdravotnícky pracovník	Odstránenie inštalácie pre ZPr	Zdravotnícky pracovník by nemal inštalovať žiadne komponenty okrem IS PZS, komponenty by malo nasadzovať NCZI. Všetky komponenty spravované NCZI by mali byť aktualizovateľné bez manuálneho zásahu.	NCZI nemá prístup na PC ZPr ani k IS PZS. Týka sa iba ambulantného ZPr.
KPI	Počet centrálnych komponentov, ktoré inštaluje ZPr	Hodnota AS IS: 2 (ovládače čítačky, cryptocontroller) Hodnota TO BE (2022):1 (bugreporting a monitoring aplikácia)	Týka sa iba ambulantného ZPr.
NCZI	Zvýšenie používania eZdravie už pripojenými ZPr	Je potrebné skrátiť trvanie incidentov Je potrebné znížiť počet incidentov Je potrebné zvýšiť používanie komponentov eZdravie	IS PZS nemajú štandardizované logovanie, je potrebné ich zjednotiť. Riešenie iba vytvára predpoklady pre používanie eReceptu. Lekári sú však motivovaný značnými úsporami času (ak nemajú technické problémy).
KPI	Zvýšenie používania podpísaného eRecept-u	Hodnota AS IS: 42% Hodnota TO BE: (2023):100%	

NCZI	Zníženie následkov incidentov	Je potrebné zrýchliť identifikáciu problému prostredníctvom analýzy logov Je potrebné rýchlejšie nasadzovať opravy na PC ZPr	NCZI nemá prístup na PC ZPr ani k IS PZS.
NCZI	Zvýšenie prevádzkyschopnosti eZdravie	Je potrebné, aby centrálne komponenty boli v správe NCZI	NCZI nemá prístup na PC ZPr ani k IS PZS. Zároveň správa komponentov musí byť podľa možností čo najjednoduchšia a automatizovaná.
Dodávateľ zdrav. softvéru IS PZS	Zníženie nákladov na implementáciu zmien eZdravie v IS PZS	Je potrebné vyňať centrálne komponenty z IS PZS (teraz sú súčasťou inštalácie)	Minimalizácia zmien v IS PZS, nakoľko zmeny predstavujú dodatočné vyvolané náklady.
KPI	Zníženie počtu aktualizácii IS PZS vyvolaných NCZI	Hodnota AS IS: 3 ročne Hodnota TO BE: (2023):1 ročne	

Riziká

Spresnenie identifikovaných rizík: *R1*

R_1 Splnenie definovaných KPI

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

n/a

Popis aktuálneho stavu

Legislatíva

Súhrnný popis

Vznik elektronického zdravotného záznamu v národnom zdravotníckom informačnom systéme je v súvislosti so zákonom č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov podmienený použitím elektronického podpisu zdravotníckeho pracovníka.

Definícia zdravotného záznamu:
Zákon 153/2013 Z.z § 2 (9).
„Elektronický zdravotný záznam je záznam zdravotníckeho pracovníka v elektronickej zdravotnej knižke vo forme elektronického dokumentu podpísaného elektronickým podpisom."

Definícia elektronického podpisu nie je daná priamo zákonom č. 153/2013 Z. z. ale je daná Nariadením E

urópskeho parlamentu a Rady č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (ďalej len „nariadenie eIDAS") a zákonom č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (ďalej len „zákon o dôveryhodných službách").
Definícia elektronického záznamu:
Nariadenie eIDAS čl.3 ods. 10- ods.15

10. elektronický podpis" sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie;

11.

„zdokonalený elektronický podpis“ je elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26;

a) je jedinečne spojený s podpisovateľom;

b) umožňuje určenie totožnosti podpisovateľa;

c) je vyhotovený pomocou údajov na vyhotovenie elektronického podpisu, ktoré môže podpisovateľ s vysokou mierou dôveryhodnosti používať pod svojou výlučnou kontrolou, a

d) je prepojený s údajmi, ktoré sa ním podpisujú, takým spôsobom, že každú dodatočnú zmenu údajov možno zistiť.

12. „kvalifikovaný elektronický podpis" je zdokonalený elektronický podpis vyhotovený s použitím kvalifikovaného zariadenia na vyhotovenie elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy;

13. „údaje na vyhotovenie elektronického podpisu" sú jedinečné údaje, ktoré podpisovateľ používa na vyhotovenie elektronického podpisu;

14. „certifikát pre elektronický podpis" je elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym;

15. „kvalifikovaný certifikát pre elektronický podpis" je certifikát pre elektronický podpis, ktorý vydáva kvalifikovaný poskytovateľ dôveryhodných služieb a ktorý spĺňa požiadavky stanovené v prílohe I

Elektronický podpis je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:
a) nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,
b) na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie,
c) obsahuje údaj, ktorý identifikuje podpisovateľa.

Elektronický podpis pre účely Národného zdravotníckeho informačného systému (NZIS) je daný elektronickým preukazom zdravotníckeho pracovníka (ePZP). Opäť zákon č. 153/2013 Z. z. definuje:

- náležitosti elektronického preukazu zdravotníckeho pracovníka
- povinnosti zdravotníckeho pracovníka požiadať si o preukaz zdravotníckeho pracovníka
- rozsah žiadosti, ktoré je NCZI oprávnené zberať pre účely výdaju preukazu zdravotníckeho pracovníka
- zánik nároku na preukaz zdravotníckeho pracovníka v súvislosti s evidenciou v komore (Zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve)
- životné situácie v súvislosti so stratou, zneužitím a poškodením elektronického preukazu zdravotníckeho pracovníka

a sankcie vyplývajúce z nedodržania vyššie uvedených povinností (Zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve)

V súvislosti s výdajom elektronického preukazu zdravotníckeho pracovníka / elektronického podpisu je NCZI certifikačnou autoritou opäť v súvislosti so zákonom od dôveryhodných službách a Nariadením eIDAS.

Riziká	**Spresnenie identifikovaných rizík:***R2*
R_2 Nestihne sa premietnuť do legislatívy, z dôvodu dlhého legislatívneho procesu	

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Architektúra

Biznis architektúra

Tabuľka 4 Biznis architektúra - aktuálny stav

Súhrnný popis

Biznis sumarizácia ePZP: v súčasnosti na prihlásenie sa do eZdravia je bez výnimky potrebná ePZP karta, ktorá sa používa na identifikáciu (kto sa prihlasuje), autentifikáciu (som to ja) ako aj autorizáciu (podpisovanie). Na plnenie týchto funkcií sa na karte nachádzajú viacere certifikáty, pomocou ktorých samotná karta podpisuje, resp. autorizuje dokumenty a úkony v systéme eZdravie. Z fyzickej povahy karty však vyplývajú viaceré obmedzenia.
Na používanie eZdravia v súčasnosti ZPr používajú svoj vlastný hardvér a softvér od komerčného dodávateľa zdravotníckeho systému, ktorý komunikuje so systémom eZdravie. NCZI však dodáva:

- čítačku ePZP kariet (v rôznych variantoch, napr. pre ambulanciu a pre lekáreň sú iné čítačky),
- softvérový komponent tzv. cryptocontroller, ktorý tvorí rozhranie medzi ePZP kartou a zdravotníckym softvérom.

Biznis sumarizácia monitoringu eZdravie: v súčasnosti NCZI disponuje monitoringom len na úrovni centrálneho systému eZdravie (NZIS) a referenčnej databázy JRÚZ. Avšak okrem zodpovednosti za prevádzku centrálneho systému eZdravie, je NCZI zodpovedné aj za prevádzku centrálnych aplikačných komponentov systému eZdravie, ktoré sú inštalované na koncovej stanici (PC) ZPr. Monitoring NCZI nepokrýva aj sledovanie koncovej stanice ZPr, tz. NCZI nevie aktívne aktualizovať aplikačné komponenty priamo na koncovej stanici ZPr v prípade nastania chyby. NCZI tak nevie riadiť opravy pri chybe samotnej aplikácie, nevie riadiť nasadenie rýchleho riešenia chyby pri globálnej aktualizácii operačného systému. Vzhľadom k tomu, že NCZI nevie monitorovať koncovú stanicu ZPr, nevie ovplyvniť dianie na koncovej stanici ZPr, ani aktívne predikovať možnú chybu a nevie predísť nastaniu incidentu. Pri aktualizáciách sa NCZI musí spoliehať na promptnosť a kapacitu samotných dodávateľov IS PZS (tj. viac ako 70 dodávateľov IS PZS). Súčasný stav má za následok najmä časovú náročnosť vyriešenia incidentu a nesystematické riadenie nasadenia riešenia.

Inštalácia komponentov ePZP a spôsobu riešenia incidentov je aj často spojená s používateľskou bázou (z hľadiska IT iba málo sofistikovanou) a je:

- zdrojom frustrácie pre ZPr, keďže miesto odbornej práce sa často krát venujú IT problémom spojeným s inštaláciou a riešením problémov,
- zdrojom negatívnej publicity spojenej s systémom eZdravie, čo aktívne bráni udržaniu počtu používateľov v systéme,
- zdrojom veľkého počtu incidentov nahlasovaných na NCZI, ktoré ale väčšinou nie je možné zo strany NCZI efektívne vyriešiť, nakoľko problém je s klientským HW/SW.

<u>Aktuálne riešenie systému eZdravie (t.j. Národný zdravotnícky informačný systém (NZIS) - ISVS_400) pre prístup ZPr do eZdravie:</u>

prostredníctvom využívania prihlasovacích kariet z pohľadu identifikácie a autentifikácie zabezpečuje identifikáciu a autentifikáciu externých používateľov NZIS, správu životného cyklu používateľov, autentizačných prostriedkov a umožňuje použitie tejto bázy informácií v informačných systémoch eZdravie, ktoré nemusia byť navzájom inak prepojené.

Riešenie tak zabezpečuje najmä :

- identifikáciu používateľov eZdravie a správu profilov ich identity,
- prepojenie subsystému IAM a procesné naviazanie, resp. automatizáciu životného cyklu identít používateľa eZdravie s integrovanými informačnými systémami,
- správu životného cyklu autentizačných predmetov (čipové karty),
- podporu jednotného prihlásenia a synchronizáciu informácií o identitách používateľov eHealth (profiloch) s replikami špecifickými pre jednotlivé informačné systémy (napr. adresárové služby, databázové úložiská, JRÚZ a pod.).

Medzi hlavné vlastnosti aktuálneho riešenia IAM patria:

- dvojfaktorová autentifikácia používateľov NZIS,
- autentifikácia je zabezpečená pomocou autentifikačnej služby (STS) vydaním SAML tokenu,
- súčasná autorizácia zo strany lekára a pacienta pri vybraných transakciách NZIS,
- karty zdravotníckych pracovníkov spĺňajú bezpečnostné požiadavky.

Používateľov NZIS možno z hľadiska identifikácie a autentifikácie rozčleniť do nasledovných základných skupín: zdravotnícky pracovník (ďalej ZPr), prijímateľ zdravotnej starostlivosti (ďalej PrZS), prevádzkový personál NCZI, výrobcov IS PKZ a IT oddelení nemocníc. Hlavný rozdiel v identifikácii a autentifikácii zdravotníckych pracovníkov a prijímateľov zdravotnej starostlivosti spočíva vo výbere autentifikačných predmetov a spôsobe ich vydávania a správy.
Identifikácia a autentifikácia ZPr je riešená priamo IAM subsystémom NZIS/eSO1. IAM subsystém z tohto pohľadu zabezpečuje:

- synchronizáciu údajov o ZPr z autoritatívneho zdroja (JRÚZ) do interného úložiska údajov pre IAM subsystém,
- prípravu autentifikačnej (nie autorizačnej) služby (STS),
- vybudovanie infraštruktúry verejných kľúčov (PKI) pre účely autentifikácie ZPr a zabezpečenie certifikátov pre elektronický (nie zaručený) podpis ZPr ako aj end-2-end transportné šifrovanie údajov na aplikačnej úrovni,
- vybudovanie technologickej infraštruktúry pre správu čipových kariet (inicializácia a potlač kariet, vydanie certifikátov, správa PIN/PUK kódov),
- prípravu klientskeho komponentu, ktorý sprostredkuje služby IAM subsystému podporovaným klientom IS PZS.

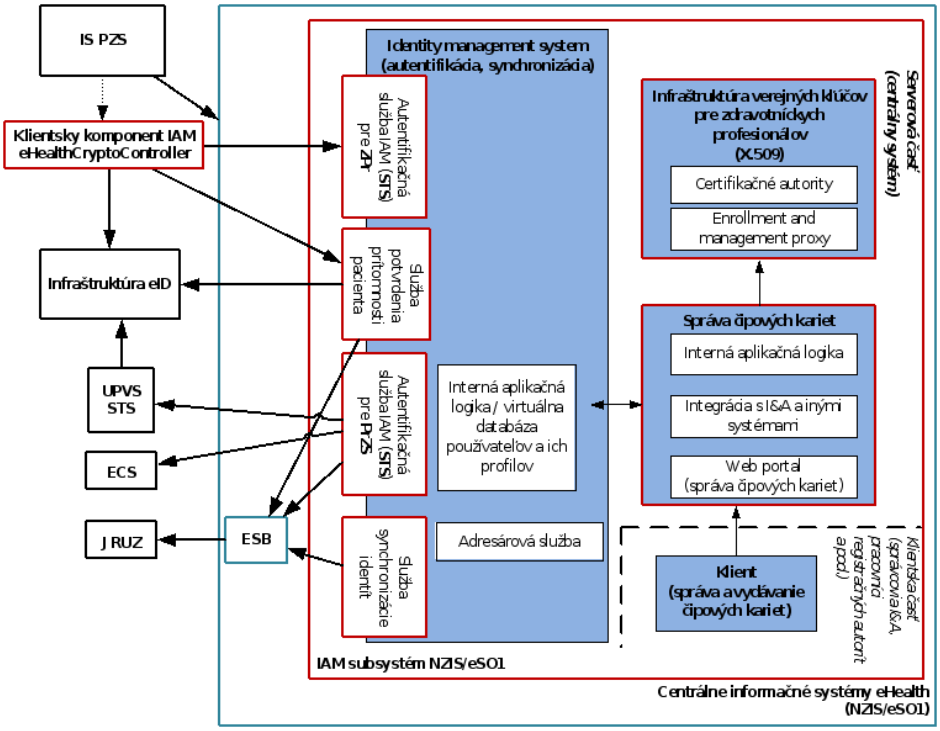
Identifikácia a autentifikácia PrZS je v rámci NZIS zabezpečená využitím elektronickej identifikačnej karty (eID). Rola IAM subsystému NZIS pri identifikácii

a autentifikácii PrZS spočíva najmä v odtienení aplikačných špecifík v smere k poskytovateľovi identity (IdP-STS) a flexibilnosti takéhoto riešenia.
IAM subsystém poskytuje dve základné služby v rámci NZIS:

- sprostredkovanie identifikácie a autentifikácie PrZS pri prístupe na webové aplikácie (napr. EZKO / NPZ) prostredníctvom internetového prehliadača. Táto časť bude realizovaná vo forme federačného scenáru, v ktorom autentifikačná služba IAM subsystému vystupuje ako R-STS a dôveruje autentifikačnej službe UPVS (IdP-STS) a eID servera Ministerstva vnútra SR.
- poskytnutie služby potvrdenia prítomnosti PrZS. Táto časť bude realizovaná vo forme webovej služby, ktorej výstupom bude podpísaný XML dokument.

Nevýhody súčasného riešenia

- Bez zasunutej karty ePZP nie je systém funkčný, čo spôsobuje, že kartu je nevyhnutné mať zasunutú po celý čas používania systému. To spôsobuje, že používateľ má kartu neustále zasunutú po celý deň.| |



Riešenie subsystému IAM NZIS je zložené z centrálnej a decentralizovaných častí. Centrálnu časť IAM riešenia tvoria nasledovné komponenty:

- infraštruktúra verejných kľúčov,
- autentifikačná služba IAM (STS) pre ZPr,
- autentifikačná služba IAM (STS) pre PrZS,
- služba potvrdenia prítomnosti prijímateľa zdravotnej starostlivosti,
- služba synchronizácie identít,
- adresárová služba,

- systém na správu čipových kariet.

Decentralizovaná časť IAM subsystému spočíva v klientskom komponente, ktorý zabezpečuje rozhrania určené na využitie služieb IAM riešenia podporovanými aplikáciami/klientmi IS PZS. Karta zdravotníckeho pracovníka obsahuje nasledovné informácie:

- X.509 certifikáty
    - Autentifikačný certifikát zdravotníckeho pracovníka
    - Certifikát pre elektronický podpis zdravotníckeho pracovníka
    - Šifrovací certifikát zdravotníckeho pracovníka
- RSA súkromné kľúče
    - Súkromný kľúč prislúchajúci k autentifikačnému certifikátu
    - Súkromný kľúč prislúchajúci k certifikátu pre elektronický podpis
    - Súkromný kľúč prislúchajúci k šifrovaciemu certifikátu

Aktuálne riešenie systému eZdravie (t.j. Národný zdravotnícky informačný systém (NZIS) - ISVS_400) pre monitoring eZdravie a aktualizáciu centrálnych komponentov:

Monitoring eZdravie:

Centrálny monitoring je aktuálne riešený na úrovni systému NZIS a databázy JRÚZ. Na úrovni NZIS sú v súčasnosti monitorované pre produkčné a pre-produkčné prostredie:

- hardvér (dostupnosť, stav a predikcia chýb)
- sieťové a bezpečnostné prvky
- operačné systémy a platformové produkty,
- aplikácie a biznis služby NZIS.

Súčasný monitoring NZIS má nasledujúce kľúčové funkcionality:

- základný monitoring,
- riadenie udalostí,
- modely služieb,
- používateľské rozhranie.

Základný monitoring – logická časť monitoringu zabezpečujúca zber a prvotné vyhodnocovanie hodnôt z monitorovacích nástrojov vo vzťahu k predmetu monitoringu. Táto logická časť:

- zbiera a vyhodnocuje fault aj performance dáta,
- zbiera a vyhodnocuje dáta na heterogénnych OS platformách,

- poskytuje základnú funkcionalitu monitoringu (state a performance monitoring), bez nutnosti dodatočného vývoja,
- zabezpečuje network discovery za účelom následnej vizualizácie sieťovej topológie,
- zabezpečuje monitoring biznis služieb z pohľadu koncového používateľa NZIS.

Riadenie udalostí – je logická časť monitornigu zabezpečujúca evidenciu a riadenie udalosti z monitoringu. Táto logická časť:

- spracováva udalostí z iných (externých) monitorovacích nástrojov,
- vyhodnocuje plánované výpadky infraštruktúry a služieb NZIS,
- spracováva a vyhodnocuje udalostí v kritických situáciách (napr. pri vygenerovaní veľkého množstva udalostí),
- vykonáva korelácie udalostí minimálne na úrovni párovania up/down správ, deduplikácie, zmeny priority na základe zdroja udalosti a času,
- automatizovaným spôsobom prenáša udalostí z monitoringu do Service Desk nástroja za účelom spracovania udalosti v rámci incident management procesu,
- identifikuje kritické udalosti na základe kritickosti zdroja udalosti (severity) a taktiež doplnkovej informácie o dopade daného zdroja na služby NZIS.

Modely služieb – je logická časť monitoringu zabezpečujúca vyhodnocovanie stavu biznis služieb NZIS na základe modelov služieb vytvorených z dostupných podkladov vo vzťahu k udalostiam vyskytujúcim sa na monitorovaných prostrediach NZIS. Pre túto logickú časť platí nasledovné:

- vyhodnocuje modely služieb NZIS na základe informácií:
    - z CMDB databázy o konfiguračných položkách a väzbách medzi nimi,
    - o udalostiach z dostupných monitorovacích nástrojov zabezpečujúcich základný monitoring,
- generuje udalosti na základe zmeny stavu monitorovanej služby, alebo jej časti,
- zohľadňuje a zobrazuje pri vyhodnocovaní modelov služieb doplnkové informácie z CMDB,

Používateľské rozhranie – je logická časť monitoringu zabezpečujúca grafické rozhranie pre prístup používateľov NCZI k jednotlivým častiam monitoringu.

Vyššie vymenované logické časti monitoringu platia len pre centrálny systém eZdravie, monitoring nepokrýva aj udalosti pre produkčné prostredie aplikácií eZdravie inštalovaných na koncovej stanici ZPr.

<u>Aktualizácia centrálnych komponentov:</u>

V prípade, ak je potrebné nasadiť aktualizáciu centrálych komponentov:

- ovládače ePZP kariet,

- ovládače ePZP čítačiek,
- ovládače eID čítačiek,
- Cryptocontroller,

NCZI v zmysle metodiky overenia zhody vydáva novú verziu integračného manuálu (slovný popis zmeny) a novú verziu samotnej aplikácie. Niektoré centrálne komponenty ako Cryptocontroller je súčasťou IS PZS a Dodávateľ IS PZS má v zmysle metodiky 60 dní n zapracovanie zmeny. NCZI teda musí maximálne 60 dní čakať na dodávateľa, kým zapracuje zmenu a následne čakať, kým aktualizovanú verziu IS PZS nasadí. Súčasný stav je nevyhovujúci, či už z pohľadu ZPr, ktorý musí na zmenu IS PZS čakať, alebo pre samotného dodávateľa IS PZS, ktorý má dodatočne vzniknuté náklady z každej jednej aktualizácie Cryptocontrollera.

Keďže Cryptocontroller je integrálnou súčasťou IS PZS (IS PZS je hrubý klient), NCZI nevie vzdialene inšlatovať aktualizácie bez potreby zásahu IS PZS. Uvedená skutočnosť predlžuje čas nasadenia a prípadných opráv problémov.

Ambulantný sektor je najpočetnejší z pohľadu počtu IS PZS, kde NCZI nemá dedikovaný tím na riešenie prípadných problémov, onsite školení a poskytovaní informácií priamo na mieste lekára alebo sestry v ambulancii. Na rozdiel, pre tzv. „veľkých PZS“, tj. nemocnice, kúpele, hospice a lekárne, kde má NCZI tím vzťahových manažérov, ktorí riešia problémy, zúčastňujú sa pravidelných stretnutí a školení a rovnako poskytujú podporu, či už pri riešení technického problému alebo pri distribúcii čítačiek. Nemocnice disponujú vlastným IT oddelením, preto samotné riešenie incidentu je svižnejšie a štruktúrovanejšie v porovnaní s ambulantným sektorom, kedy lekár nedokáže identifikovať a popísať technický problém, nevie poskytnúť logy zo systému a nepozná riešenie IT architektúry.

Pre ambulantný sektor neexistuje koncepčné riešenie nahlasovania incidentov priamo pri nastaní incidentu a to priamo z koncovej stanice ZPr. Pre ZPr existuje call centrum/helpdesk NCZI, na ktorý môžu zavolať ZPr s problémom ohľadne eZdravie. Problémy so samotným zdravotníckym softvérom rieši helpdesk, resp. kontakt príslušného dodávateľa (tento proces je znázornený aj v procesných mapách v prílohe CBA).

Pri nastaní incidentu ambulantný ZPr väčšinou nahlasuje chybu na call centrum NCZI, pretože nevie správne identifikovať, či sa jedná o chybu na strane IS PZS alebo je chyba spôsobená centrálnym systémom. NCZI na základe telefonátu častokrát nevie vyrrišiť chybu, pretože na to potrebuje detailnejšie technické informácie, ktoré ZPr nevie poskytnúť. Pravidlá pre integráciu IS PZS do eZdravie síce definujú požiadavku na logovanie všetkých udalostí na úrovni IS PZS, ZPr však nevie, kde sa tieto logy v počítači nachádzajú a preto ich nevie proaktívne poskytnúť NCZI pre rýchlejšie vyriešenie incidentu.

Nemocnice na rozdiel od ambulancií majú centrálne pripojenie do ezdravie za celú nemocnicu prostredníctvom SSL pripojenia alebo VPN routera, rovnako nemocnica disponuje špecializovaným nástrojom, cez ktorý vedia hromadne aktualizovať všetky PC v sieti nemocnice.

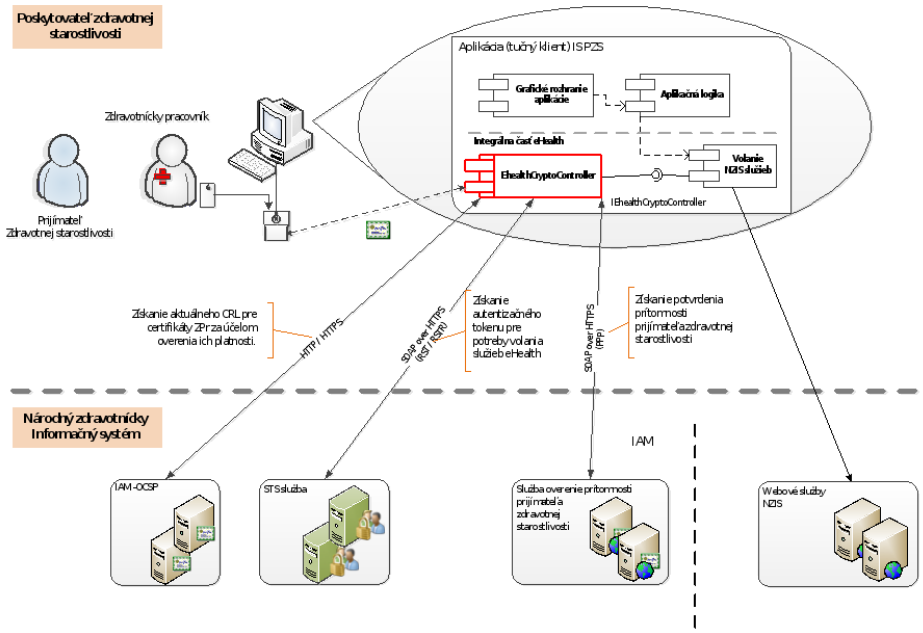
Riziká	Spresnenie identifikovaných rizík:*Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
R_8 Pri zachovaní súčasného stavu riešenie nedosiahne požadované zachovanie penetrácie pripojenia a tým pádom ciele projektu R_9 Nie je možné v budúcnosti rozšíriť na mobilné platformy	
Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**

Architektúra informačných systémov

Tabuľka 5 Architektúra informačných systémov - aktuálny stav

Súhrnný popis

Kľúčovou oblasťou celého eZdravia v rámci tejto štúdie je práve subsystém IAM a interakcia tohto subsystému a klientskych časti riešenia. Z pohľadu klientskeho prostredia v systéme NZIS je kľúčovým komponentom práve „EhealthCryptoController".
Komponent tvorí modulárnu súčasť priamo tučného klienta IS PZS a zabezpečuje potrebnú interakciu tohto klienta s centrálnymi časťami IAM subsystému ako sú napríklad služby autentizácie a overenia prítomnosti PrZS. Rovnako zastrešuje potrebnú interakciu s čítacím zariadením čipových kariet a X.509 certifikátmi uloženými na týchto kartách.
Komponent EhealthCryptoController je fyzicky umiestnený na pracovnej stanici ZPr, na ktorej sa spúšťa tučný klient IS PZS a ku ktorej je pripojené čítacie zariadenie čipových kariet. Priamo z tejto pracovnej stanice komponent realizuje aj potrebnú sieťovú komunikáciu s centrálnymi časťami IAM subsystému.



Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „ApplicationUsageViewpoint", „ApplicationCo-operationViewpoint"

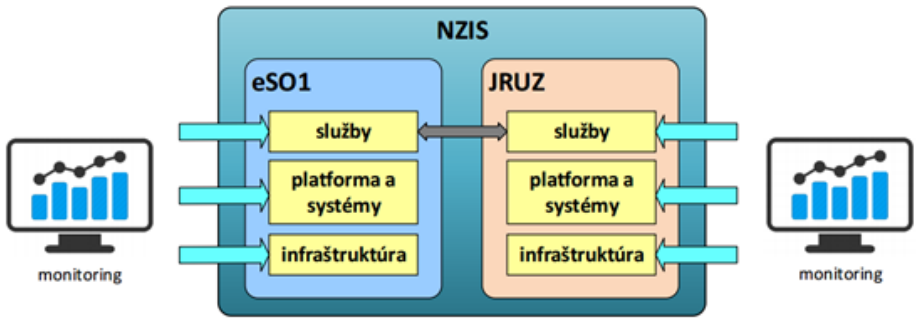
Z hľadiska monitoringu je v aktuálnom riešení pre komunikáciu na službách využívaná jednotná dátová štruktúra. Na najvyššej úrovni je správa definovaná štruktúrou eHTalkMessage. Teda už v rámci týchto správ sú logované nasledujúce sady údajov:

- Jednoznačný identifikátor správy,
- Údaje o type správy a odosielateľovi,
- Údaje o identite, ktorá správu odoslala a v mene koho ju odoslala,
- a iné.

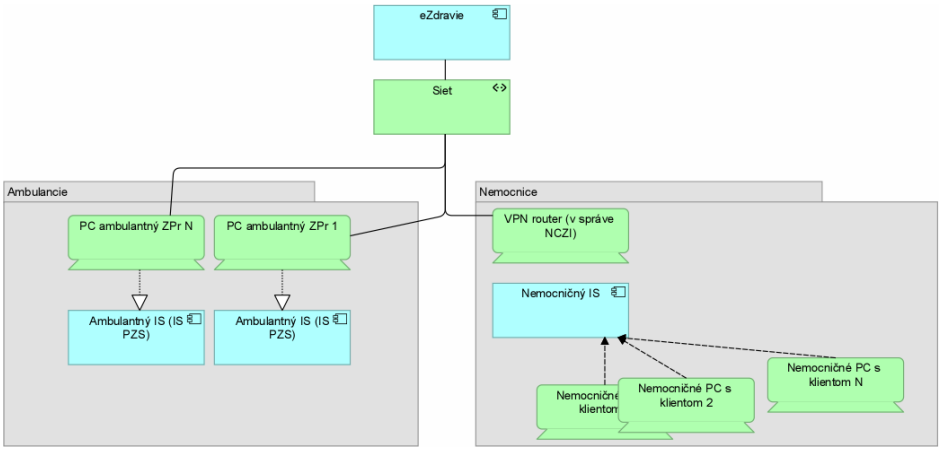
Na sieťovej úrovni sú všetky správy logované, logy sú nahrávané do centrálneho syslog riešenia. Monitoring centrálneho (serverového) riešenia dokáže:

- zberať a vyhodnocovať fault aj performance dáta,
- zberať a vyhodnocovať dáta na heterogénnych OS platformách,
- poskytnúť základnú funkcionalitu monitoringu (state a performance monitoring), bez nutnosti dodatočného vývoja,
- zabezpečiť network discovery za účelom následnej vizualizácie sieťovej topológie,
- zabezpečiť monitoring biznis služieb z pohľadu koncového používateľa NZIS,
- vykonávať korelácie udalostí minimálne na úrovni párovania up/down správ, deduplikácie, zmeny priority na základe zdroja udalosti a času,
- automatizovaným spôsobom prenášať udalostí z monitoringu do Service Desk nástroja za účelom spracovania udalosti v rámci incident management procesu,
- identifikovať kritické udalosti na základe kritickosti zdroja udalosti (severity) a taktiež doplnkovej informácie o dopade daného zdroja na služby NZIS.

Na nasledovnom obrázku je členenie systému po vrstvách a je tu znázornený aj vzťah na monitoring:



Rozdielny spôsob pripojenia nemocníc a ambulancií je znázornený na nasledovnom obrázku:



Riziká

Stručná charakteristika identifikovaných rizík (Max. 400 znakov)

R_10 Nedostatočná automatizácia
R_11 Nízke využívanie služieb vzhľadom na neposkytovanie moderných služieb

Spresnenie identifikovaných rizík:*Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

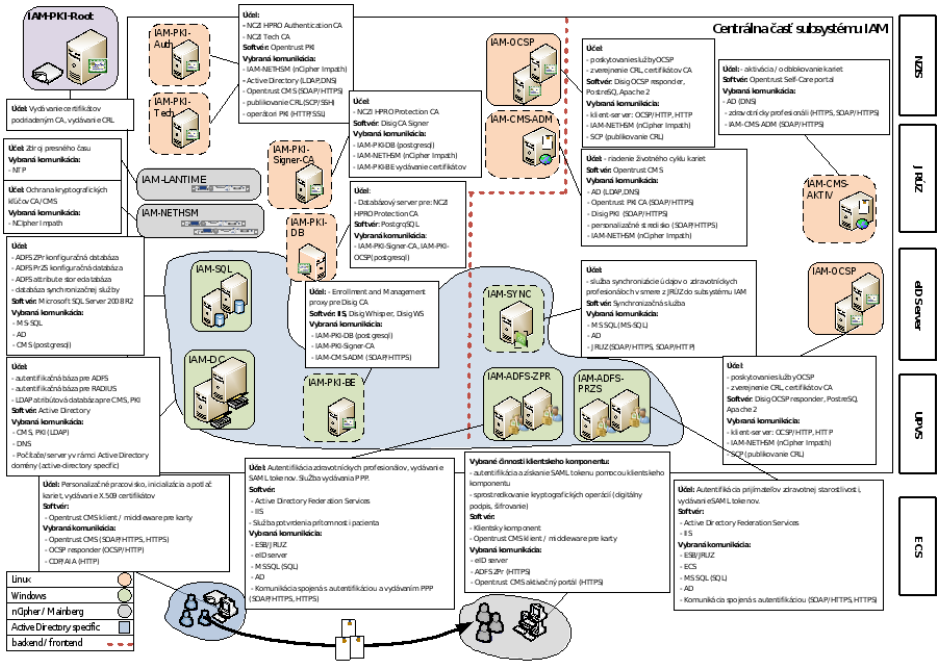
Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Technologická architektúra

Tabuľka 6 Technologická architektúra - aktuálny stav

Súhrnný popis

Úvodné informácie
Technologickú architektúru komponentov v rámci IAM subsystému ilustruje nasledujúci obrázok. Uvedený obrázok sumarizuje informácie týkajúce sa technologických platforiem a ilustruje ich vzájomné prepojenie.



Z hľadiska monitoringu je nasadený funkčný modul "Umbrella monitoring", ktorý je založený na rodine produktov IBM Tivoli:

- ITM (IBM Tivoli Monitoring) – agentský monitoring pre Linux/Windows platformu,
- ITNM (IBM Tivoli Network Manager) – SNMP monitoring siete a HW zariadení,
- IBM NCOB (Netcool/OMNIbus) – online objektová databáza udalostí,
- IBM TBSM (Tivoli Business Service Manager) – monitoring biznis služieb,
- IBM DB2 – databázový systém IBM DB2,
- IBM JazzSM DASH – WebGUI rozhranie pre IBM Tivoli produkty,
- IBM TCR (Tivoli Common Reporting) – aplikácia pre štatistické reporty z UM.

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Riziká

Spresnenie identifikovaných rizík:*Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

Stručná charakteristika identifikovaných rizík (Max. 400 znakov)

N/A

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

Bezpečnostná architektúra

Tabuľka 7 Bezpečnostná architektúra - aktuálny stav

Súhrnný popis

IAM subsystém pre zabezpečenie bezpečnej prevádzky spĺňa nasledovné technologické a organizačné opatrenia:

- Dohľadové centrum: riešenie disponuje centrálnym dohľadovým centrom (SIEM / kontrola audit logov).
- Konfigurácia riešenia sa po nasadení nemení (konfigurácia RP ADFS, profily PKI, profily CMS, a pod.).
- Prístupové práva sú prideľované v súlade s princípom minimálnych právomocí (tzn. nepoužívajú sa účty s právami Administrator (Windows) a root (Linux) pre bežnú prevádzku a správu).
- Rozdelenie rolí prevádzky a správy IAM infraštruktúry je prispôsobené tak, že dopad bezpečnostného incidentu impersonifikácie ZPr je potenciálne nebezpečnejší ako výpadok riešenia (kompromis medzi prevádzkou a bezpečnosťou riešenia je realizovaný v prospech bezpečnosti riešenia).
- Fyzická a sieťová bezpečnosť bráni útokom MitM v rámci serverovej infraštruktúry. Pozn.: v rámci sieťovej komunikácii sa používajú bezpečné protokoly
- Osoby zodpovedné za správu a prevádzku IAM nedokážu modifikovať nastavenia sieťovej infraštruktúry (konfigurácia FW, prepínačov a smerovačov).
- V prípade virtualizovaných serverov je operátor hostiteľského servera kritická rola a preto je riešenie nastavené tak, že hostiteľský server sa nedá konfigurovať vzdialene (analógia s fyzickým prístupom ku serveru).
- Prevádzkové a administračné úkony sú vykonávané odlišnými osobami (separácia prevádzky a administrácie).

- V procesoch je organizačne zabezpečené, že osoby sa nedokážu vydávať za niekoho iného, napr. ak sa vyžaduje overenie podpisu riaditeľa prevádzky, vzor podpisu / pečiatky riaditeľa prevádzky je zamestnancom známy.
- V rámci infraštruktúry je k dispozícií SMTP server prístupný z vybraných serverov IAM subsystému, účelom tohto SMTP servera je zasielanie notifikácií (aplikačné a systémové notifikácie).

IAM subsystém v rámci prevádzky plní nasledovné opatrenia:

- Ochrana kryptografických kľúčov certifikačných autorít a komponentov ktoré majú dosah na impersonifikáciu ZPr je zabezpečená prostredníctvom HSM
- Kryptografické kľúče uložené v HSM sú chránené pomocou administrátorských kariet v schéme k/n, k>1, tzn. nie je možné spraviť obnovu HSM Security World na inom HSM jedinou osobou
- Kryptografické kľúče certifikačných autorít, OCSP responderov a autentifikačných serverov (STS) uložené v HSM sú chránené pomocou operátorských kariet

Úvodná inštalácia a konfigurácia IAM subsystému prebehla v kontrolovaných podmienkach s ohľadom na bezpečnosť. Presný postup je súčasťou prevádzkovej dokumentácie, ktorá z tohto pohľadu pokrýva okrem iného:

- postupy pri inštalácii aplikačného vybavenia certifikačných autorít,
- postupy pri generovaní (opis ceremoniálu) kryptografických kľúčov certifikačných autorít,
- záznam / zápis o generovaní kryptografických kľúčov certifikačných autorít, autorizovaný vlastníkmi operátorských kariet,
- postupy pri úvodnej konfigurácii APV certifikačných autorít a systému na správu čipových kariet.

Bezpečnostná architektúra monitoringu je založená na kontrole prístupu pomocou nasledovných faktorov:

- prístup k monitoringu je zabezpečený pomocou VPN, s autentizáciou do VPN pomocou certifikátu umiestneného na SMART karte vystavenej pre konkrétneho používateľa,
- používatelia musia cez webový prehliadač s autentifikáciou voči ich doméne,
- iba prístupový komponent sa nachádza v perimetrovej časti siete.

Priestor pre sumárny obrázok / graf / diagram.

Riziká

Spresnenie identifikovaných rizík:*Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

Stručná charakteristika identifikovaných rizík (Max. 400 znakov)

N/A

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Prevádzka

Tabuľka 8 Prevádzka - aktuálny stav

Súhrnný popis

IAM Subsystém je jeden z najdôležitejších modulov národného zdravotníckeho informačného systému (NZIS). Prevádzka tohto modulu je zabezpečená spolu s ostatnými modulmi riešenia ako aj ďalšími podpornými systémami NZIS. Jedná sa o tieto systémy:

- správa a prevádzka národného zdravotníckeho informačného systému (NZIS),
- správa a prevádzka Call Centra pre NZIS,
- správa a prevádzka webového sídla NPZ,
- bezpečnosť prevádzky NCZI ako správcu a prevádzkovateľa NZIS.

Všetky tieto riešenia v správe NCZI sú prevádzkované ako vysoko dostupné riešenie v režime 24x7 s nasledovnými SLA parametrami:

- Dostupnosť systému 98%,
- Výpadky – max 175 hodín ročne pričom max 15 hodín mesačne (súčet časov trvania incidentov typu A),
- dĺžka podpory 36 mesiacov + opcia na ďaľších 12 mesiacov.

Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.

Riziká

Spresnenie identifikovaných rizík:*Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

R_12 Prevádzka súčasného riešenia je nákladná z hľadiska podpory používateľov

R_13 Nedostatočná forma dodávateľskej podpory môže mať za následok dlhšie odstraňovanie problémov

R_14 Nedostatočné pokrytie internými pracovníkmi môže viesť k zdržaniu riešenia problémov

Prílohy

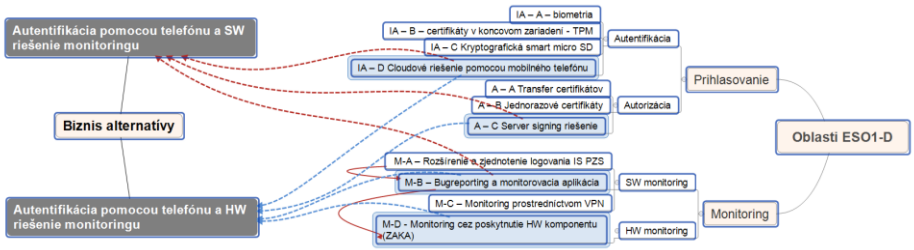
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Alternatívne riešenia

Biznis sumarizácia: Vzhľadom na technickú tému a pomerne veľké množstvo dostupných možností riešenia sa v štúdii v časti Alternatívne riešenia najprv rieši aplikačná a technologická architektúra. Obe oblasti štúdie (mobilné ePZP a monitoring) majú svoje technologické alternatívy a svoju mini MCA, pomocou ktorej sú vybrané možné technické varianty. Z týchto možných technických variantov je následne možné vytvoriť biznis alternatívy, ktoré sú potom predmetom samostatnej MCA. Celý postup vrátane jednotlivých alternatív je znázornený na nasledovnom obrázku:



Legenda: technologický prípustné alternatívy sú znázorené modrou farbou. Uvažované biznis alternatívy sú znázornené sivou farbou, pričom čiarované čiary znázorňujú priradenie technických alternatív do biznis alternatív. Červené čiary ukazujú, že jedna alternatíva je súčasťou ďalšej alternatívy.

Alternatívne možnosti prihlasovania

Alternatívne riešenia Identifikácie a autentifikácie pre eZdravie

Štúdia uskutočniteľnosti navrhuje niekoľko alternatív riešenia, ktoré by mohli riešiť súčasný neoptimálny stav. Pri identifikácií alternatívnych riešení identifikácie a autentifikácie pre eZdravie predpokladáme, že používateľ bude aj naďalej na prístup k eZdraviu používať počítač s príslušným zdravotníckym softvérom. Pre prvú časť - identifikácia a autentifikácia ZPr – oblasť 1 (alternatívny spôsob identifikácie a autentizácie zdravotného pracovníka bez použitia ePZP karty),
Z toho vyplývajú nasledovné skutočnosti spoločné pre všetky alternatívy:

- identifikácia a autentifikácia môžu prebiehať nezávisle od HW a SW vybavenia PC používateľa,
- po úspešnej identifikácií a autentifikácií musí existovať proces, ktorým sa umožní prístup PC používateľa k systému eZdravie, čo technicky znamená, že musí:
    - existovať spôsob ako stiahnuť certifikát a zodpovedajúci privátny kľúč na definované typy certifikátov,
    - existovať bezpečný kanál na doručenie kľúčov, alebo
    - existovať spôsob podpisovania na serveri bez samotného prístupu k privátnym kľúčom (server signing).

Celkové riešenie teda bude kombináciou:

- identifikácie a autentifikácie,
- spôsobu autorizácie a prenosu kryptografických kľúčov.

Súčasný spôsob autentizácie používateľa do eZdravia je založený na využití kryptografického materiálu (páru kľúčov), pričom:

1. kľúčový pár je generovaný v bezpečnom prostredí (v čipe karty ePZP)
2. privátny kľúč je chránený PINom
3. privátny kľúč je celú dobu chránený (neopúšťa čip)

Čip slúži ako bezpečné zariadenie na generovanie a uchovávanie kľúčov. Je vložený do plastového obalu – karty a prostredníctvom čítačky čipových kariet cez USB rozhranie pripojený k počítaču používateľa.

Z uvedených princípov je nutné vychádzať aj pri definovaní potenciálnych alternatív, aby nedošlo k nežiadúcemu zníženiu bezpečnostnej úrovne riešenia. Vo všeobecnosti do úvahy pripadajú nasledovné možnosti:

1. nahradiť čip karty ePZP a súčasný spôsob autentifikácie pomocou infraštruktúry PKI prostredníctvom biometrie
2. nahradiť čip karty ePZP iným druhom čipu (napr. TPM, micro SD karty a pod.), ktorý sa bezkáblovo pripojí k mobilnému zariadeniu,
3. nahradiť čip karty ePZP centralizovaným cloudovým riešením (bezpečné generovanie a centralizovaný manažment kryptografických kľúčov, bez nutnosti existencie ďalšieho zariadenia)

Je však potrebné si uvedomiť, že využívanie mobilného zariadenia (prevažne mobilný telefón/smartfón) so sebou vždy bude prinášať aj riziká, či už vo forme nebezpečných aplikácií, rootnutého OS a pod., kedy ani seba lepšie šifrovanie nemusí z povahy využitia bezpečnostných slabín samotného mobilného zariadenia znamenať neprelomiteľnú ochranu spracovávaných dát. Tieto bezpečnostné riziká by však mali byť riadne identifikované a v rozumnej miere minimalizované doplňujúcimi bezpečnostnými opatreniami.

Všetky riešenia by mali spĺňať požiadavky vykonávacieho nariadenia Komisie (EÚ) 2015/1502 – úroveň Vysoká.

IA – A – biometrické údaje

Táto alternatíva predstavuje dvojfaktorovú identifikáciu a autentifikáciu, kde používateľ musí preukázať niečo čo má (biometrický údaj za účelom identifikácie) a niečo čo vie (PIN za účelom autorizácie). Možnosti biometrickej identifikácie prichádzajú do úvahy nasledovné:

- krvné riečište,
- dúhovka,
- odtlačok prsta.

Výhodou tejto alternatívy je, že používateľ nemusí so sebou mať žiadne technické zariadenie. Nevýhodou je nutnosť vybaviť všetky pracoviská hardvérom na skenovanie príslušného biometrického parametra a s ním súvisiace inštalácie potrebného SW vybavenia a jeho integrácie s IS lekárov v závislosti od podporovaných OS. Taktiež bude potrebné vyriešiť plošnú registráciu zdravotníckych pracovníkov. Do úvahy prichádzajú priestory NCZI alebo priestory IOM (ktoré by sa tiež museli vybaviť potrebným HW). Nevýhodou tejto alternatívy je, že obsahuje množstvo osobných údajov a keďže pôjde o osobitnú kategóriu OÚ, treba implementovať prísne opatrenia v zmysle nariadenia GDPR.
Rizikom je spoločenské odmietnutie vytvorenia centrálneho registra pre zber a správu biometrických údajov

IA – B – certifikáty v koncovom zariadení - TPM

V tejto alternatíve sa uvažuje s priblížením certifikátov k používateľovi, tak aby nemusel nosiť kartu s certifikátmi a identifikoval a autentifikoval sa menom a heslom.
Používateľov je možné rozdeliť na dve skupiny:

- „statická" používatelia, ktorí pracujú primárne so svojím zariadením, typicky ambulantní lekári,
- „ dynamická" používatelia, ktorí v priebehu pracovnej doby vystriedajú viacero pracovísk, typicky sú to lekári v nemocniciach.

Pre statických používateľov je možné certifikáty distribuovať priamo na ich PC do bezpečného úložiska, ktoré je podporované operačným systémom Windows.
Využitie kryptografického úložiska operačného systému používateľa na uloženie súkromných kľúčov a X.509 certifikátov však nepredstavuje dostatočne bezpečnú alternatívu, nakoľko táto konfigurácia je zraniteľná rovnakými útokmi ako sú zraniteľné operačné systémy.
Vyššiu úroveň bezpečnosti predstavuje kombinácia softvérového úložiska s TPM čipom, pričom až táto alternatíva predstavuje bezpečnosť porovnateľnú s fyzickou kartou. V tejto alternatíve teda ďalej uvažujeme iba so zabezpečením prostredníctvom TPM čipu. Výhody zabezpečenia pomocou TPM sú nasledovné:

- nie je možný export certifikátov,

- funkcia zablokovania po definovanom počte nesprávnych pokusov o zadanie PIN,
- izolácia kľúčov od operačného systému – operácie s certifikátmi sa realizujú priamo v TPM.

Nevýhodou TPM čipu je jeho minimálna trhová penetrácia. s rizikom zvýšenia nákladov na zaobstaranie si PC s vybaveným TPM modulom pre zdravotníckeho pracovníka.
V prípade nemocníc je potrebné realizovať dynamickejšie riešenie, ktoré umožní mobilitu lekárov, čo je možné realizovať pomocou HSM modulu.

Pre prvú časť - identifikácia a autentifikácia ZPr – oblasť 2 (identifikácia a autentizácia zdravotného pracovníka prostredníctvom mobilného zariadenia)

IA – C Kryptografická smart micro SD

Táto alternatíva uvažuje s vydávaním certifikátov a kvalifikovaných certifikátov a uložením kryptografických kľúčov na Smart Micro SD karty, ktoré by spĺňali požiadavky bezpečného úložiska kľúčov a bolo by možné ich použiť v mobilných zariadeniach platforiem Windows Phone a Android. Nevýhodou riešenia je jednak nemožnosť pripojiť Smart MicroSD k mobilným zariadeniam so systémom iOS inak než externou čítačkou a nutnosť nákupu kariet pre každé mobilné zariadenie zvlášť. Navyše vznikne potreba novej agendy manažovania a distribúcie ďalšieho zariadenia (mikrokarty, resp aj čítačky).

V čase prípravy dokumentu nebola žiadna Smart Micro SD karta certifikovaná ako bezpečné zariadenie Národným bezpečnostným úradom SR,, ani sa v blízkej dobe nepredpokladá, že by niektorý z výrobcov o takúto certifikáciu požiadal. Z uvedeného dôvodu vyplýva, že táto alternatíva nebude umožňovať využitie autorizácie KEPom. Pre jej využitie by tak okrem zaistenia prístupnosti pre všetky mobilné platformy bola aj nutnosť certifikácie karty ako bezpečného zariadenia pre elektronický podpis, čo nie je pravdepodobné.

Obrázok č. 1 – Smart micro SD karta

IA – D *Cloudové riešenie pre mobilnú identifikáciu a autetifikáciu*

Táto možnosť predstavuje centralizované cloudové riešenie (bezpečné uloženie a centralizovaný manažment kryptografických kľúčov), ktoré je postavené na jednorazovej registrácii používateľa (napr. prostredníctvom ePZP karty, vytvorení jeho virtuálnej identity v centrálnom bezpečnom úložisku využívajúcom certifikované kryptografické zariadenia a digitálne certifikáty rovnakej úrovne ako na sú na ePZP karte, jednorazovom spárovaní mobilného zariadenia s centrálnym bezpečnostným úložiskom a následnom plnohodnotnom využívanie služieb identifikácie a autentifikácie bez potreby akéhokoľvek dodatočného zariadenia. Riešenie je možné v prípade

zvýšenej požiadavky na bezpečnosť doplniť o viacfaktorový autentizačný systém. V súčasnej dobe už existujú riešenia (aj certifikované Národným bezpečnostným úradom SR resp. inými uznávanými medzinárodnými inštitúciami), vrátane možnosti využívania KEPu pre potreby autorizácie používateľov.

Výhodou tohto riešenia je najmä:

· jeho použiteľnosť v širokom spektre mobilných zariadení (min. Android, iOS).

· centralizované riešenie vhodné pre cloudové prostredie

· po úvodnej registrácii nevyžaduje už žiadny ďalší token, čip, čítačka, kábel ani iné zariadenie – iba spárované mobilné zariadenie, prostredníctvom ktorého sa používateľ bude prihlasovať do systému

· vysoká úroveň ochrany (certifikovaný HW aj SW)

Nevýhodou tohto riešenia je najmä potreba udržiavania SW vybavenia pre viaceré platformy (min. Android, iOS), keďže pre každú platformu je potrebné vytvoriť a následne udržiavať samostatnú aplikáciu.

Alternatívne možnosti autorizácie

Autorizácia v kontexte eZdravia znamená podpisovanie, šifrovanie a dešifrovanie údajov. Bez ohľadu na možnosti identifikácie a autentizácie zdravotníckeho pracovníka (oblasť 1 aj 2) za účelom vykonania týchto aktivít je potrebné mať k dispozícii sadu privátnych a verejných kľúčov, ktoré sa v súčasnosti nachádzajú na fyzickej čipovej karte. Keďže v novom riešení karta nie je podmienkou autorizácie, je potrebné:

- dostať kryptografické kľúče na zariadenie používateľa
- vykonávať autorizáciu mimo zariadenia používateľa
- dostať kryptografické kľúče do centrálneho bezpečného úložiska

Uvedené možnosti sú popísané ako alternatívy nižšie, pričom sú kombinovateľné s už uvedenými možnosťami identifikácie a autentifikácie.

Z biznis pohľadu je možné možnosti popísať nasledovne:

- A – A Transfer certifikátov bezpečnou cestou používateľovi - jedná sa o nahratie certifikátov z karty na počítač PZS. Teda neboli by na karte, ale na PC. Problémom je ako ochrániť tieto ciertifikáty pred zneužitím - na to slúži čip TPM, ktorý ale nie je štandardnou súčasťou PC. Museli by sa teda nakupovať nové, pričom bezpečnostné riziko by aj tak nebolo úplne eliminované.
- A – B Jednorazové certifikáty - alternatíva predstavuje generovanie jednorazových certifikátov, ktoré by sa bezpečnou cestou kopírovali na zariadenie PZS. Keďže certifikát by mal obmedzenú platnosť, nebolo by potrebné vyžadovať TPM čip.

- A – C Server signing riešenie - alternatíva predstavuje riešenie, kde sú certifikáty uložené na serveri, kde aj prebieha šiforovanie, dešifrovanie a podpisovanie. Na aktiváciu týchto funkcií je požadovaná iba identifikácia a autentifikácia. Výhodou serverového riešenia je, že ho stačí implementovať centrálne, na jednotlivých zariadeniach už nie je funkcionalitu potrebné nasadzovať.

A – A Transfer certifikátov bezpečnou cestou používateľovi

Táto alternatíva predstavuje možnosť, kedy sa kryptografické kľúče dostanú na zariadenie používateľa. Základné podmienky bezpečného využívania tejto alternatívy sú nasledovné:

- bezpečné úložisko certifikátov – v prípade trvalých certifikátov na úrovni TPM,
- bezpečný transfer certifikátov šifrovanou cestou (po identifikácii a autentifikácii).

Akonáhle sú certifikáty na zariadení používateľa, je možné ich využiť obdobným spôsobom ako sú využívané certifikáty na fyzickej čipovej karte. Samozrejme, bude musieť byť modifikovaný crypto controller, aby podporoval aj inú lokalitu certifikátov ako na fyzickej čipovej karte.
Pri tejto alternatíve prichádza do úvahy aj použitie jednorazových certifikátov, kedy by nemuseli byť nároky na úložisko také vysoké. Po autentifikácii by serverový komponent na zariadenie neposlal trvalé certifikáty, ale jednorazové pre danú session – čo je v podstate analógia k tokenom pri webových službách.
Podmienkou samozrejme je vybudovanie infraštruktúry pre uloženie kryptografických kľúčov pre ePodpis a realizáciu kryptografických funkcií elektronického podpisu.
Z pohľadu bezpečnosti si takéto riešenie vyžaduje prijatie najmä prísnejších organizačných a personálnych opatrení vrátane pravidelných a nepravidelných auditov a rôznych kontrol, najmä v oblasti riadenia prístupov (fyzických aj logických) a v oblasti správy a vyhodnocovania logov a auditných záznamov.

A – B Jednorazové certifikáty

Táto alternatíva predstavuje možnosť, kedy sa jednorazové kryptografické kľúče s krátkou časovou platnosťou dostanú na zariadenie používateľa. Základné podmienky bezpečného využívania tejto alternatívy sú nasledovné:

- bezpečné úložisko certifikátov – bez nutnosti TPM,
- bezpečný transfer certifikátov šifrovanou cestou (po identifikácii a autentifikácii).

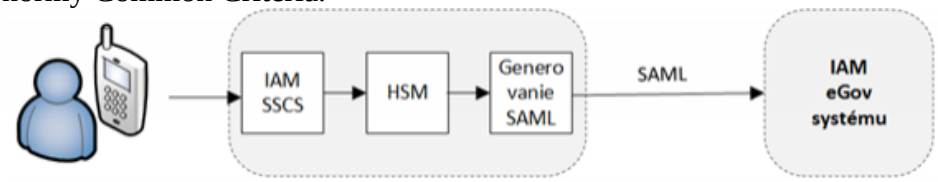
Akonáhle sú certifikáty na zariadení používateľa, je možné ich využiť obdobným spôsobom ako sú využívané certifikáty na fyzickej čipovej karte. Samozrejme, bude musieť byť modifikovaný crypto controller, aby podporoval aj inú lokalitu certifikátov ako na fyzickej karte.
Podmienkou samozrejme je vybudovanie infraštruktúry pre uloženie kryptografických kľúčov pre el. podpis a realizáciu kryptografických funkcií elektronického podpisu.
Z pohľadu bezpečnosti si takéto riešenie vyžaduje prijatie najmä prísnejších organizačných a personálnych opatrení vrátane pravidelných a nepravidelných auditov a rôznych kontrol, najmä

v oblasti riadenia prístupov (fyzických aj logických) a v oblasti správy a vyhodnocovania logov a auditných záznamov.

A – C Server signing riešenie

Osobitnú formu autorizácie predstavuje tzv. Server signing riešenie, ktoré funguje na princípe tzv. centralizovaného serverového systému podpisovania. Server Signing riešenie (SSCS – Secure Signature Creation Service) vychádza z požiadaviek normy CEN/TS 419241:2014 – Security Requirements for Trustworthy Systems Supporting Server Signing. Systém by umožnil používateľom generovanie kľúčového páru a následné vydanie certifikátov priamo v centrálnom úložisku na strane NCZI. Táto alternatíva predpokladá vytvorenie riešenia na báze centrálneho bezpečného úložiska kľúčov pre elektronický podpis a funkcionality pre elektronické podpisovanie elektronických dokumentov- (spĺňa to napr. IA – D Cloudové riešenie pre mobilnú identifikáciu a autetifikáciu).

Okrem podpisovania by systém bol využívaný aj na ostatné funkcie, ktoré v súčasnosti realizuje cryptocontroller.
Funkcionalitu tohto systému zo strany používateľov je možné využívať v podstate okamžite po jeho vytvorení a uvedení do prevádzky, bez dodatočných nákladov na strane používateľov.
Požiadavky Výnosu o štandardoch pre ISVS v oblasti úrovní autentifikácie predpokladajú použitie uznávaného bezpečného autentifikačného mechanizmu poskytujúceho ochranu pred všetkými útokmi, ktorými sú uhádnutie, odpočúvanie siete, únos relácie, útok typu odpoveď a muž v strede, a to najmenej na úrovni Evaluation Assurance Level 4 (EAL4+) podľa technickej normy Common Criteria.



Podmienkou samozrejme je vybudovanie infraštruktúry HSM modulov pre uloženie kryptografických kľúčov pre ePodpis a realizáciu kryptografických funkcií (prípade aj kvalifikovaného) elektronického podpisu.
Z pohľadu bezpečnosti si takéto riešenie vyžaduje prijatie najmä prísnejších organizačných a personálnych opatrení vrátane pravidelných a nepravidelných auditov a rôznych kontrol, najmä v oblasti riadenia prístupov (fyzických aj logických) a v oblasti správy a vyhodnocovania logov a auditných záznamov.

Vzhľadom na existujúci stav a skúsenosti s využívania infraštruktúry PKI a HSM modulov v rámci systému eZdravie by takéto riešenie nemalo spôsobovať žiadne dodatočné nároky a problémy tak v personálnej ako prevádzkovej oblasti.

Technická multikriteriálna analýza - autentifikácia a autorizácia

Tabuľka 9 Technická multikriteriálna analýza - autentifikácia a autorizácia

Kritérium	**Nutné**	IA-A	IA-B	IA-C	IA-D	A-A	A-B	A-C
Bezpečnosť	áno	áno	áno	áno	áno	áno, s rizikom	áno	áno
Jednoduchý deployment	áno	nie	nie	nie	áno	áno	áno	áno
Jednoduchá implementácia		nie	nie	áno	áno	áno	áno, s rizikom	nie
Spĺňajú súčasné zdrav. SW predpoklady riešenia		áno	áno	áno	áno	áno	áno	nie
Potenciál rozšíriteľnosti medzi lekárov	áno	áno	áno	nie	áno, s rizikom	áno	áno	áno
Jednoduchosť použitia	áno	áno	áno, s rizikom	áno	áno	áno	áno	áno
Jednoduchosť administrácie a prevádzky		nie	áno	áno, s rizikom	áno	nie	áno	áno
Rýchlosť použitia		-	-	-	-	áno	áno	áno
Neobsahuje osobné údaje		áno	áno	áno	áno	áno	áno	áno
Odolnosť voči malvéru a vírusom		áno	nie	nie	áno	nie (iba v kombinácii s TPM)	áno	áno
Riešenie je multiplatformné, t. j. do budúcnosti podporuje aj MacOS, Linux a mobilné platformy	áno	áno	nie	nie	áno	nie	áno, s rizikom	áno

Vysvetlivky: hodnoty boli určené na základe požiadaviek stakeholderov, prieskumov, následného expertného odhadu a vzájomných konzultácii s NCZI.

Technické kombinácie alternatív

Jednotlivé alternatívy riešenia identifikácie, autentifikácia a autorizácie predstavujú iba čiastkové riešenia, ktoré je potrebné skombinovať. Teoreticky je možné všetky tri možnosti autorizácie kombinovať s možnosťami riešenia identifikácie a autorizácie, prakticky (prihliadnuc aj na výsledky MKA) však do úvahy prichádzajú najmä nasledovné možnosti:

- IA-B certifikáty v koncovom zariadení uložené v TPM a alt. A-A transfer certifikátov bezpečnou cestou,
- IA-D SW token v telefóne a aplikácia v kombinácii s:
    - A-A transferom certifikátov bezpečnou cestou používateľovi,
    - A-B jednorazovými certifikátmi,
    - A-C server signing riešením.

S prihliadnutím na výsledky MKA sa ako najvhodnejšia javí alternatíva IA-D spolu s A-C, t. j. softvérový token v mobilnom zariadení a server signing riešenie (t. j. presun funkcií cryptocontrollera do serverovej časti).

Alternatívne riešenia monitoringu

Riešenie monitoringu má riešiť nasledovné biznis problémy, ktoré vyplynuli zo skúseností z prevádzky a podpory súčasného systému. Jedná sa o:

- konektivita – veľa lekárov má nespoľahlivé, alebo nesprávne nakonfigurované internetové pripojenie, čoho si lekári vysvetľujú ako nefunkčnosť systému eZdravia ako takého,
- deployment a inštalácia – z pohľadu najmä starších lekárov (ktorí tvoria nezanedbateľnú časť používateľov) je inštalácia centrálnych aplikačných komponentov problém. Ak sa jedná o viacero inštalácii, tak kombinácia nižšej používateľskej zdatnosti, množstva PC konfigurácii a zložitosti inštalácie je často problémom.
- monitoring – cieľom NCZI je proaktívne monitorovať infraštruktúru eZdravia a mať prehľad o stave všetkých komponentov najmä v prípade nahlásenia problému od používateľa, ako aj za účelom sledovania trendov a proaktívneho riešenia vzniknutých problémov so systémom.

V prípade monitoringu sú uvažované nasledovné alternatívy, z hľadiska prehľadnosti a čitateľnosti uvádzame ich biznis sumarizáciu:

- Alternatíva M-A – „Rozšírenie a zjednotenie logovania IS PZS" predstavuje získavanie záznamov z počítača ZPr jednotným spôsobom. IS PZS by samozrejme museli zjednotiť spôsob zápisu logov a všetky typy IS PZS by museli ukladať logy na rovnaké miesto. V prípade problému by následne používateľ tieto logy poslal na analýzu do NCZI.
- Alternatíva M-B – „Rozšírenie funkcionality komponentu eZdravia o monitoring zariadenia ZPr a kvality pripojenia na eZdravie" predstavuje implementáciu aplikácie, ktorá umožní nahlasovať incident na NCZI, pričom by automaticky priložila aj logy na analýzu. ZPr si bude môcť online pozrieť stav svojej požiadavky, resp. incidentu.
- Alternatíva M-C – „Rozšírenie a zjednotenie logovania IS PZS a využívanie VPN pripojenia" predstavuje využitie funkcionality pripájania pomocou klienta VPN, ktorý by bol využitý na získanie informácii a logov z počítača ZPr. V súčasnosti sa však na pripripojenie do systému využíva protokol na báze SSL, čo spôsobuje, že alternatíva nie je priamo použiteľná pre všetkých ZPr.
- Alternatíva M-D – "Poskytnutie nakonfigurovaného komunikačno-autentifikačného modulu zdravotníckym pracovníkom" predstavuje softvérové riešenie a inštanciu komunikačno-autentifikačného modulu, ktorý by sa pripájal na počítač lekára a do siete eZdravia. Tým by bolo zabezpečené, že celá prístupová cesta ZPr do eZdravie by bola pod správou NCZI, ktoré by zabezpečovalo jej funkčnosť.

Alternatíva M-A – „Rozšírenie a zjednotenie logovania IS PZS"

Súhrnný popis

V aktuálnom riešení eZdravia v prípade zasielania údajov z IS PZS do NZIS systém informuje odosielateľa správy buď o tom, že jeho správa sa zapísala korektne alebo v prípade neúspechu zašle relevantné chybové hlásenie.
Zaslaním akejkoľvek správy z IS PZS do NZIS a v prípade jej prijatia, sa na strane NZIS vytvorí záznam v zozname logov, kde sú uložené všetky potrebné informácie ohľadom predmetnej správy. V niektorých prípadoch už aj tieto systémové logy dokážu zefektívniť komunikáciu a riešenie problémov, ktoré zdravotnícky pracovníci nahlasujú na helpdesk.
Pre úplne zastrešenie agendy, aplikačná a prevádzková podpora NZIS a riešenie vzniknutých incidentov, v rámci tejto alternatívy navrhujeme nadefinovať spoločnú sadu atribútov, ktoré je potrebné logovať v prípade akéhokoľvek IS PZS. Taktiež je potrebné nadefinovať spôsob v akých časových intervaloch budú tieto logy zasielané do NZIS a akým spôsobom budú tieto údaje párované s príslušnými systémovými logmi evidovanými v rámci NZIS.
Za zváženie v rámci tejto alternatívy taktiež stojí možnosť automatického naviazania zasielaných logov IS PZS na evidované a riešené incidenty v rámci service desku.

Aplikáciou alternatívy rozšírených a jednotných logov IS PZS je možné takto získané údaje využívať napr. aj na vyhodnotenie a vytvorenie predikcií určitých problémov. Napr. keď sa v poslednom čase stalo, že posledných 10 zápisov laboratórneho vyšetrenia zo zariadenia s daným OS s verziou updatu XY neprešlo, je vysoká pravdepodobnosť, že tento update nie je kompatibilný a je potrebné riešiť tento všeobecný problém ešte skôr ako bude zaevidovaných ďalších X rovnakých incidentov.

Navrhované riešenie je z nášho pohľadu minimálna množina aktivít a zmien, ktoré je nevyhnutné vykonať na to, aby sa zefektívnil spôsob monitorovania koncových používateľov a ich zariadení v rámci riešenia eZdravia. Všetky nasledujúce nami navrhované alternatívy sú v podstate len rozšírenie tejto alternatívy o ďalšie funkcionality a komponenty.

Túto variantu sme vyhodnotili ako nepostačujúcu pre komplexné riešenie problematiky, nakoľko stále bude prevládať problém s rôznorodosťou hardvérového a softvérového vybavenia koncových zariadení na strane zdravotníckym pracovníkov a implementácia jednotnej štruktúry logov do IS poskytovateľov je z nášho pohľadu značný zásah do mnohých IS s minimálnou pridanou hodnotou, nakoľko tým nezabezpečíme zníženie počtu incidentov v rámci využívania eZdravia, ale len efektívnejšie riešenie vzniknutých incidentov. Rovnako sa nezabezpečí manažment aplikačných komponentov systému eZdravie inštalovaných na koncovej stanici ZPr.

Alternatíva M-B – „Rozšírenie funkcionality komponentu eZdravia o monitoring zariadenia ZPr a kvality pripojenia na eZdravie"

Súhrnný popis

V aktuálnom riešení eZdravia v prípade, že sa chce PZS integrovať na NZIS musí využívať v rámci svojho zariadenia bezpečnostný komponent EHealthCryptoController, ktorý zabezpečuje bezpečnú komunikáciu medzi predmetným IS PZS a NZIS. Jedna z alternatív je rozšíriť funkcionalitu tohto komponentu prípadne vytvoriť podobný komponent, ktorý bude schopný v prípade potreby zaslať určitú sadu údajov, ktorá by s vysokou pravdepodobnosťou postačovala na odhalenie systémových nedostatkov komunikácie IS PZS a NZIS.
Nový komponent môže byť navrhnutý tak, aby umožňoval vytvárať a odosielať žiadosť o službu na základe vzniknutých incidentov prípadne porúch, počas využívania eZdravia priamo na kontaktné centrum NCZI. Prílohou takto definovanej a odoslanej správy môže byť aj systémový súbor, obsahujúci sadu informácií o SW a HW vybavení zariadenia, z ktorého je žiadosť odosielaná.
Pre kompletné pokrytie agendy aplikačná a prevádzková podpora eZdravia a riešenie vzniknutých incidentov v rámci tejto alternatívy navrhujeme zvážiť aj možnosti integrácie tohto komponentu s nástrojom na riešenie incidentov na strane kontaktného centra NCZI. Integráciou by sa zabezpečilo to, že jednotlivé žiadosti od používateľov eZdravia by boli automaticky zaevidované v rámci nástroja Service Desk. Tieto žiadosti by samozrejme obsahovali omnoho viac technických informácií ako sú schopný koncový používatelia (ZPr) nahlásiť v prípade telefonického kontaktu s kontaktným centrom.
V rámci tejto alternatívy je možné navrhovaný komponent rozšiť aj o jednoduché GUI rozhranie pre ZPr, kde by si v prehľadnej forme mohol pozrieť svoju aktivitu v rámci eZdravia. Teda napr.

- koľko a akých záznamov posiela na eZdravia,
- aká je úspešnosť ich zasielania,
- koľko trvá zaslanie správy na strane IS PZS a koľko trvá spracovanie správy v rámci eZdravia,
- koľko trvá vyriešenie jeho žiadosti o službu,
- a iné (rozhranie na helpdesk a pod.).

Výhodou tohto riešenia je najmä podpora a zefektívnenie procesu nahlasovania incidentov ako aj zrýchlenie doby riešenia týchto problémov. Ďalšou výhodou je, že pokiaľ by sa tieto problémy ZPr nahlasovali prostredníctvom na to určenej aplikácie a obsahovali by okrem samotného popisu problému aj dostatočnú sadu technických údajov predmetného zariadenia a spojenia, doba riešenia incidentov by sa určite zrýchlila. Z pohľadu samotných ZPr by sa aplikáciou tohto riešenia zefektívnila a zjednodušila komunikácia smerom na NCZI. V prípade implementácie modulu na strane ZPr pre zobrazovanie jeho aktivity v rámci eZdravia, by malo toto riešenie určite priaznivý vplyv na informovanosť jednotlivých ZPr a v prípade potreby sa môže toto riešenie využiť aj na informovanie ZPr o mimoriadnych situáciách a prípadných odstávkach systému.

Táto alternatíva spĺňa požiadavky kladené na monitoring a prináša aj pridanú hodnotu pre samotných zdravotníckych pracovníkov nakoľko by mali prehľad o svojej aktivite v rámci systému eZdravia. Dôvod, prečo sme nezvolili túto alternatívu je, že akákoľvek inštalácia na koncovú stanicu ZPr je pre pracovníkov NCZI veľmi obtiažna, nakoľko ZPr buď nemá počas svojich ordinačných hodín priestor alebo odmieta inštaláciu akýchkoľvek aplikácii na svoj počítač (poväčšine viac dôveruje svojmu dodávateľovi IS PZS, ktorý je väčšinou aj správcom počítača ZPr). Rovnako dôvod, prečo sme nezvolili túto alternatívu je kvôli procesu riešenia vznikajúcich incidentov a faktu, že nerieši prevádzkové problémy. V nami navrhovanom riešení by všetky incidenty smerovali hneď od zdravotníckeho pracovníka priamo do service desku prevádzkovateľa NZIS. V aktuálnom riešení tieto incidenty riešia na úrovni L1 poskytovatelia IS a až v prípade, že sú zadané incidenty preverené a súvisia s prevádzkou NZIS, tak sú presmerované do kontaktného centra NCZI.
Neriešené prevádzkové problémy sa preukazujú predovšetkým v ambulanciách, kde je veľmi heterogénne HW a SW prostredie, čo vedie k problémom s prevádzkou (ktorú používatelia často krát pripisujú eZdraviu, aj keď sa jedná o lokálny problém). Najmä z dôvodu nedostatočné riešenia tejto skutočnosti nebola táto alternatíva vybraná.

Alternatíva M-C – „Rozšírenie a zjednotenie logovania IS PZS a využívanie VPN pripojenia"

Súhrnný popis

V prípade, že IS PZS využije na spojenie s NZIS pripojenie prostredníctvom VPN a aplikácie Cisco AnyConnect Secure Mobility Client, tak už týmto spôsobom je zabezpečený prístup k určitej sade informácií potrebných na riešenie prípadných incidentov a nekonzistencií v komunikácií. V spojení VPN pripojenia a zjednoteného logovania definovaného v alternatíve A je možné vytvoriť riešenie, ktoré umožní automatické ukladanie logov na strane IS PZS do špecifikovaného súboru, ktorý môže byť vďaka špecifickej konfigurácii VPN pripojenia prístupný zo strany dohľadového centra. Týmto riešením je zabezpečené, že v prípade nahlásenia nejakého incidentu zo strany ZPr využívajúceho VPN pripojenie je možné získať všetky potrebné logy priamo z dostupného súboru a tak využiť technické informácie logov pre efektívne vyriešenie predmetného problému.

Výhodou tohto riešenia je fakt, že už v rámci aktuálneho systému je možné pre spojenie s NZIS využiť spomínané VPN pripojenie a teda nie je nutná žiadna ďalšia úprava funkcionality.

Táto alternatíva je z pohľadu požiadaviek zákazníka na pripojenie do systému NZIS neprípustná nakoľko väčšina ZPr preferuje pripojenie prostredníctvom zabezpečeného SSL protokolu a nie sú ochotní inštalovať si na svoje koncové zariadenia VPN klienta.

Alternatíva M-D – "Poskytnutie nakonfigurovaného komunikačno-autentifikačného modulu zdravotníckym pracovníkom"

Súhrnný popis

V tejto alternatíve navrhujeme možnosť poskytnúť zdravotníckym pracovníkom predkonfigurovaný autentifikačno-komunikačný modul (KAM), ktorý bude vyrobený a nastavený presne tak, aby spĺňal všetky požiadavky na prácu v ambulantnom prostredí. KAM by poskytovalo vo forme softvéru alebo samostatnej inštancie spôsob, akým sa ZPr pripája do Systému eZdravie. KAM inštancia nepredstavuje, ani nenahradzuje počítač lekára, ale predstavuje inštanciu pripojenú k počítaču lekára a predstavuje tak komunikačno-autentifikačný modul medzi počítačom ZPr a Systémom eZdravie. Za prevádzku KAM by bolo v plnej miere zodpovedné NCZI. Pre tých ZPr, ktorí by nepožadovali inštanciu a chceli by inštalovať centrálne komponenty sami, by NCZI poskytlo práve softvérovú verziu SW. V rámci analýzy budúceho stavu NCZI vykonalo prieskum a preberalo možnosť umiestnenia inštancie KAM u ambulantných lekárov. Tí podporili alternatívu inštancie KAM a zámer tohto riešenia. Ako jednu z výhod riešenia uviedli úsporu času venovanému nahlasovaniu incidentov, riešenie incidentov na strane ZPr a zníženie času pre nasadenie nových verzií.

Inštancia KAM a KAM-sw by bolo určené predovšetkým pre ambulantný sektor mimo nemocníc, pretože nemocnice majú vlastnú správu sietí a koncových staníc, teda disponujú vlastným IT oddelením, ktoré dokáže efektívne nastávajúce incidenty riešiť (pričom však KAM-sw je možné po otestovaní nasadiť aj v nemocniciach). Inštancia KAM je preto určené práve pre ambulantný sektor, kde je veľmi heterogénne dodávateľské prostredie, ako aj HW a SW prostredie v ambulanciách, čo vedie k problémom s prevádzkou eZdravie na strane NCZI.

Aplikáciou inštancie KAM by sa zabezpečilo, že zmeny a vplyvy vonkajšieho prostredia, tj. prostredia, ktoré NCZI nevie ovplyvniť (napr. aktualizácia Windows) by boli minimálne, až nulové, pretože inštancia by mala vlastný image a správa všetkých aktualizácii by bola riadená NCZI. V ambulatnom sektore je ešte stále využívaná nepodporovaná a zastaralá verzia OS Windows XP (37 percent), čo môže spôsobiť postupné znemožnenie pripojenia do eZdravie - niektoré aplikačné komponenty eZdravie nepodporujú alebo v blízkej dobe nebudú podporovať Windows XP. Práve z tohto dôvodu je potrebné centrálne komponenty umiestniť z počítača ZPr do KAM.
Požiadavky na KAM sú, aby tento modul bol vyrobený presne podľa požiadaviek trhu a NCZI, aby bolo možné Systém efektívne prevádzkovať v ambulantnom prostredí. Taktiež je potrebné zo strany NCZI, alebo jeho subdodávateľa, ešte pred samotným spustením KAM do prevádzky správne nakonfigurovať a nainštalovať všetky nevyhnutné komponenty do KAM, ktoré zabezpečia bezproblémovú komunikáciu medzi modulom a systémom eZdravie. Následne po prevzatí KAM bude mať zdravotnícky pracovník k dispozícii všetky prerekvizity pre kontinuálne a bezproblémové pripojenie do systému eZdravie. Súčasťou alternatívy je aj softvérové riešenie KAM-sw - samostatný program, ktorý bude mať rovnakú funkciu ako kompletná inštancia KAM, t.j. bude jednoducho inštalovať a automaticky aktualizovať komponenty, ktoré dodáva NCZI. Softvér bude poskytovať lokálne sieťové služby.

Pre IS PZS by malo byť transparentné, prípadne iba vecou konfigurácie, či používa inštanciu KAM, alebo KAM-sw, služby budú poskytovať iba na inej IP adrese.

Aplikáciou tejto "D" alternatívy by sa odbúrali mnohé administratívne a prevádzkové problémy, nakoľko by boli všetky inštancie KAM a KAM-sw v správe prevádzkovateľa eZdravia, tj. NCZI, ktorý by takto zabezpečilo jednotnú konfiguráciu všetkých modulov a následne by

zabezpečovalo aj ich prípadnú aktualizáciu. Využívaním modulu by sa značne vyriešil čas potrebný na opravy a aktualizácie, ZPr by mal k dispozícii nástroj na reportovanie incidentov, NCZI by malo prehľad o aplikačných komponentoch a vedelo by tak rýchlo a efektívne riadiť nasadenia opráv, predikovať problém a poskytovať tak väčšiu podporu pre samotných ZPr.

Požiadavky na inštanciu KAM budú bližšie špecifikované v rámci analýzy riešenia. Rámcovo ich však je možné určiť nasledovne:

- integrálnou súčasťou inštancie KAM sú čítačky ePZP a eID kariet,
- integrálnou súčasťou inštancie KAM je aj čítačka kódov (napr. kód elektronického receptu, kód výmenného lístka a pod.),
- viacero sieťových výstupov umožňujúcich pripojenie k počítaču ZPr a do eZdravie
- obsahuje predinštalované nasledovné centrálne kompomenty:
    - ovládače ePZP kariet,
    - ovládače ePZP čítačiek,
    - ovládače eID čítačiek,
    - Cryptocontroller.

KAM inštancia a KAM-sw neobsahujú ambulantný softvér PZS, t.j. počítač lekára je naďalej nevyhnutný pre používanie zdravotníckeho softvéru a eZdravie. Inštancia KAM nenahrádza počítač lekára ani nie je jeho alternatívou.

Na predkonfigurovaných inštanciách KAM by bol software centrálne monitorovaný a manažovaný prostredníctvom dedikovaného tímu, ktorý bude zabezpečovať:

-
    -
        - monitoring
        - sledovanie stavu KAM, aplikácia bude nahlasovať stav zariadenia na centrálne miesto,
            - vzdialená správa ovládačov a centrálnych komponentov eZdravie,
            - distribúciu a prípadné onsite zásahy,
            - inventarizácia centrálnych aplikácií.
        - deployment aplikácii,
            - možnosť vzdialenej inštalácie a správy centrálnych aplikácii eZdravie, prípadná vzdialená reinštalácia
            -
            - inštalácia a správa software-u.
        - bugreporting
            - zber logov z relevantného časového úseku z event logu, prípadne z IS PZS možnosť sledovať riešenie chyby a hlasovať o jednotlivých už nahlásených chybách (na spôsob user voice),
            - troubleshooting problémov a diagnostika,
            - automatická distribúcia chýb do centrálneho logu NCZI,

        - možnosť pre ZPr hlasovania o chybách a návrhoch na zlepšenie centrálneho riešenia,
        - možnosť pre ZPr poslať chybové hlásenie, ktoré bude obsahovať relevantné logy,
        - možnosť pre ZPr popísať prípadný popis chyby,
        - možnosť pre ZPr získať prehľad o stave Systému eZdravie,
    -
        -
        - tracking riešenia chyby, zobrazovanie riešenia chyby pre ZPr.
    - reporting:
        - možnosť sledovať štatistiky vlastnej session ZPr a celkové štatistiky centrálneho systému eZdravie,
        - stav centrálneho systému Systému eZdravie (healthcheck stránka).

Softvérové riešenie KAM-sw bude plniť nasledovné rámcové požiadavky:

- jednoduchá inštalácia a priebežná automatická aktualizácia komponentov:
    - ovládače ePZP kariet,
    - ovládače ePZP čítačiek,
    - ovládače eID čítačiek,
    - Cryptocontroller,
- zmena komponentov tak, aby poskytovali lokálne sieťové služby, analogické s KAM.

Táto alternatíva má aj vyvolané náklady súvisiace s potrebnou zmenou IS PZS. Tieto požiadavky ako aj náklady sú analyzované v návrhu TO BE stavu.

Hlavnou výhodou tohto riešenia je možnosť jednoduchšieho deploymentu aplikačných komponentov eZdravie (ZPr odmieta sprístupnenie svojho počítaču pre NCZI za účelom inštalácie aplikácií alebo nie je ochotný počas ordinačných hodín sprístupniť počítač). Celoplošnou aplikáciou tejto alternatívy v ambulantnom sektore by bolo zabezpečené, že väčšina počítačov ZPr, ktoré komunikujú so systémom eZdravia, by využívalo len také aplikačné komponenty, ktoré sú plne kompatibilné a aktuálne s celým riešením eZdravia. Týmto riešením by sa minimalizovali situácie, kedy budú vznikať incidenty. V prípade vzniku nejakého incidentu, bude zo strany NCZI veľmi jednoduché dohľadať KAM, identifikovať, kde tento problém nastal a vďaka vzdialenej správe KAM tento incident okamžite odstrániť resp. aspoň identifikovať príčinu a zahájiť ďalšie aktivity na jeho odstránenie. Oproti Alternatíve A je výhodou tohto riešenia fakt, že v rámci rozšírenia a zjednotenia logovania na strane IS PZS sa v tejto alternatíve stačí zamerať len na zjednotenie logovania jednotlivých IS PZS a nie je potrebné riešiť akékoľvek iné SW a HW komponenty počítaču ZPr, lebo tie sú pre NCZI známe.

Dôvod zamietnutia, alebo výberu riešenia (Max. 400 znakov)
Zo všetkých navrhovaných alternatív najkomplexnejšie pokrýva predmetnú problematiku alternatíva D, nakoľko jej realizáciou zabezpečíme plnú správu, riadenie a dohľad NCZI nad KAM a centrálnymi komponentmi eZdravie. Ďalšou výhodou tejto alternatívy je efektívnejšie riešenie vzniknutých incidentov, nakoľko KAM budú v správe prevádzkovateľa eZdravie príp. jeho subdodávateľa, ktorý vďaka vzdialenej správe KAM môže incident okamžite odstrániť resp. aspoň identifikovať príčinu a zahájiť ďalšie aktivity na jeho odstránenie.

Zároveň táto alternatíva D prostredníctvom SW riešenia umožnuje minimalizáciu nákladov na inštancie, pokiaľ to bude možné.

Čiastočnou nevýhodou tohto riešenia je komplexnosť a potreba fyzickej distribúcie, inštalácie a následnej správy inštancií KAM (čo je náročnejšie ako v prípade KAM-sw).

Technická multikriteriálna analýza - monitoring

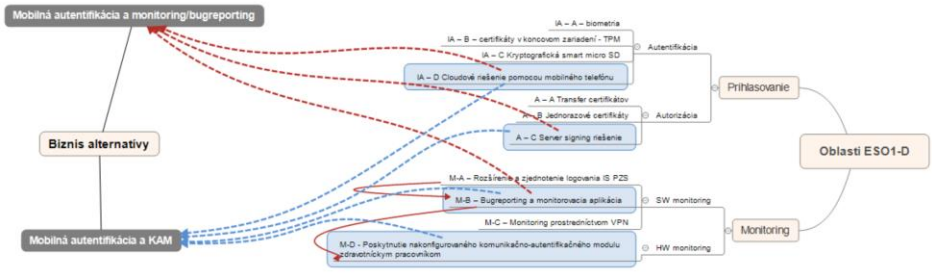
Tabuľka 10 Technická multikriteriálna analýza - monitoring

Kritérium	KO	A	B	C	D
Bezpečnosť	áno	áno	áno	áno	áno
Jednoduchá inštalácia z pohľadu lekára	áno	áno	áno	áno, s rizikom	áno
Jednoduchá správa a deployment	áno	nie	áno	áno	nie
Možnosť remote aktualizácie		nie	áno	áno, s rizikom	áno
Konfigurovateľnosť monitorovania		áno	áno	nie	áno
Riešenie konektivity		nie	nie	nie	áno

Vysvetlivky: hodnoty boli určené na základe požiadaviek stakeholderov, prieskumov a následného expertného odhadu a konzultácii s NCZI.

Výber alternatívy

Z analýzy technických alternatív je vyplynuli možné technické riešenia, ktorých kombinácie je potrebné analyzovať z biznis pohľadu. Celá situácia tvorby biznis alternatív je znázornená na nasledovnom obrázku:



Alternatíva A: Mobilná autentifikácia a predstavuje navrhované riešenie prihlasovania (identifikácie, autentifikácie a autorizácie) spolu s riešením monitoringu ambulantných IS PZS prostredníctvom bugreportingovej a monitorovacej aplikácie, ktorá by sa inštalovala na PC ZPr. Riešenie neobsahuje KAM.

Alternatíva B: Mobilná autentifikácia a KAM rozširuje alterantívu A o samostatný modul mimo PC ZPr s vlastným image, ktorý je v plnej správe NCZI a nie je ovplyvnený zmenami na PC lekára.

Biznis multikriteriálna analýza

Tabuľka 11 Multikriteriálna analýza

	Kritérium	Zdôvodnenie kritéria	Zdravotnícky pracovník	NCZI	Dodávateľ IS PZS
Biznis vrstva	Zavedenie alternatívnej identifikácie a autentifikácie (nutné)	Kritérium prinesie: • Zvýšenie komfortu lekára • Rýchlejší prístup k eZdravie v prípade straty ePZP • Umožní mobilné riešenia, t.j. prístup mobilných ZPr do eZdravie	X	X	X

	Kritérium prinesie:		
Zavedenie aktívneho monitorovania a bugreportingovej aplikácie (nutné)	• Zrýchlenie zadávania incidentov pre ZPr • Lepšiu infomovanosť lekárov o vlastných štatistikách používania eZdravie a aktuálnom stave eZdravie • Lepšiu kvalitu a dostupnosť monitorovacích údajov a logov z IS PZS	X	X

Zavedenie inštancie KAM pre komunikáciu a autentifikáciu (preferované)	Kritérium prinesie: • Zrýchlenie odstraňovania incidentov • Zabezpečenie modulu pred zmenami vonkajšieho prostredia • Zjednodušenie nasadzovania zmien centrálnych komponentov u ZPr • Proaktívnu a rýchlu identifikáciu problému centrálnych komponentov u ZPr • Úsporu nákladov dodávateľa IS PZS	X	X	X
Zníženie následkov incidentov - rýchlejšie opravy chýb (preferované)	Rýchlejšie odstraňovanie chýb bude viesť k: • zníženiu odchodov ZPr z eZdravie, • lepšiemu napĺňaniu pôvodných prínosov eZdravie.	X	X	X

Centrálne komponenty v správe NCZI (preferované)	Ak budú centrálne komponenty v správe NCZI, zvýši sa prevádzkyschopnosť IS eZdravie, keďže NCZI bude vedieť rýchlejšie identifikovať problém a nasadiť jeho opravu.	X	X	
Automatické aktualizácie lokálnych komponentov eZdravie (preferované)	Automatické aktualizácie vyriešia najmä problém častého nasadzovania zmien Cryptocontrollera, ktorý je teraz súčasťou IS PZS. Každá zmena cryptocontrollera teda znamená novú verziu IS PZS, pričom doba nasadenia zmeny je 60 dní. Pri automatických aktualizáciach by už Cryptocontroller nebol súčasťou IS PZS a bol by aktualizovaný automaticky.		X	X
Jednoduchá a rýchla inštalácia komponentov (preferované)	Veľa problémov ZPr je spôsobených náročnou inštaláciou centrálnych komponentov na PC ZPr. Zjednodušením inštalácie sa zvýši miera používania eZdravie.	X		

	Jednoduché nasadenie riešenia (či už z pohľadu NCZI alebo lekára) zvyšuje dlhodobú pravdepodobnosť úspechu			
Jednoduchosť riešenia (preferované)	Jednoduchosť riešenia je jeden z uznávaných architektonických konceptov (KISS), ktorý zvyšuje pravdepodobnosť dodania riešenia v rámci jeho časových, finančných a funkčných obmedzení	X	X	X
Bezpečnosť (nutné)	Vzhľadom na typ údajov, ktoré sa v systéme nachádzajú je bezpečnosť neodmysliteľnou súčasťou kritérií navrhovaného riešenia.		X	X

Tabuľka 12 Multikriteriálna analýza - vyhodnotenie

Zoznam kritérií	**Alternatíva A**	**Spôsob dosiahnutia**	**Alternatíva B**	**Spôsob dosiahnutia**
Zavedenie alternatívnej identifikácie a autentifikácie	áno	Zavedením druhého faktora pomocou mobilného telefónu a server signing riešenia na autorizáciu	áno	Zavedením druhého faktora pomocou mobilného telefónu a server signing riešenia na autorizáciu
Zavedenie aktívneho monitorovania a bugreportingovej aplikácie	áno	Vytvorením špecifickej aplikácie, ktorá sa bude inštalovať na PC ambulantného ZPr.	áno	Vytvorením špecifickej aplikácie, ktorá sa bude inštalovať na PC ambulantného ZPr.

Zavedenie modulu pre komunikáciu a autentifikáciu - inštancia KAM	nie		áno	Vytvorením custom inštancie KAM, ktorý sa bude nasadzovať u ambulantných ZPr a bude slúžiť ako proxy.
Zníženie následkov incidentov - rýchlejšie opravy chýb	čiastočne	Rýchlejším nahlásením aj s logami IS PZS a centránych komponentov bude možné rýchlejšie identifikovať chybu.	áno	Rýchlejším nahlásením aj s logami IS PZS a centránych komponentov bude možné rýchlejšie identifikovať chybu. Zároveň bude možné rýchlejšie nasadiť opravu chyby.
Centrálne komponenty v správe NCZI	nie		áno	Centrálne komponenty by sa nachádzali v KAM, ktorá je v správe NCZI.
Automatické aktualizácie lokálnych komponentov eZdravie	nie		áno	NCZI vie aktualizovať komponenty v KAM automaticky, bez ľudského zásahu na mieste.
Jednoduchá a rýchla inštalácia komponentov	nie		áno	V prípade vysunutia centrálnych komponentov do KAM už ich nie je potrebné inštalovať na PC ZPr.
Jednoduchosť riešenia	áno	Riešenie obsahuje iba SW komponenty, pričom princíp jednoduchosti bol súčasťou návrhu.	nie	Riešenie obsahuje aj HW časti, ktoré je potrebné vyvinúť, nasadiť a spravovať.
Bezpečnosť	áno	Riešenie je navrhnuté s ohľadom na bezpečnosť údajov.	áno	Riešenie je navrhnuté s ohľadom na bezpečnosť údajov.

Obe alternatívy spĺňajú nutné kritériá, preto boli posúdené aj z hľadiska nákladov a prínosov v CBA. Z tohto posúdenia lepšie vychádza alternatíva B, ktorá má síce vyššie náklady, avšak aj rádovo vyššie prínosy. Detaily tohto porovnania sa nachádzajú v kapitole CBA a v samotných CBA prílohách.

Popis budúceho stavu

Legislatíva

Tabuľka 11 Legislatíva - budúci stav

Súhrnný popis

Vznik elektronického zdravotného záznamu v národnom zdravotníckom informačnom systéme je v súvislosti so zákonom č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov podmienený použitím elektronického podpisu zdravotníckeho pracovníka.

Definícia zdravotného záznamu:
Zákon 153/2013 Z. z § 2 (9).
„Elektronický zdravotný záznam je záznam zdravotníckeho pracovníka v elektronickej zdravotnej knižke vo forme elektronického dokumentu podpísaného elektronickým podpisom."

Definícia elektronického podpisu nie je daná priamo zákonom č. 153/2013 Z. z. ale je daná Nariadením Európskeho parlamentu a Rady č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (ďalej len „nariadenie eIDAS") a zákonom č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (ďalej len „zákon o dôveryhodných službách").
Definícia elektronického záznamu:
Nariadenie eIDAS čl.3 ods. 10- ods.15
Do zákona č.153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov je potrebné pridať formuláciu :„ a ďalšie možnosti autentifikácie" a zároveň aj o„ mobilnú aplikáciu".
Doplnenie ePZP karty bude potrebné riešiť aj zmenou legislatívy - zákona č. 153/2013 Z. z.(Elektronický podpis pre účely Národného zdravotníckeho informačného systému (NZIS) je daný elektronickým preukazom zdravotníckeho pracovníka (ePZP).)

Do vyhlášky MZSR o materiálno-technickom vybavení ambulancií č. 09812/2008-OL je potrebné doplniť ako povinnú výbavu ambulancií "komunikačno-autentifikačný modul".

Kritéria kvality

Legislatívne zmeny v MPK

Spresnenie kritérií kvality: *Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.*

Riziká

R_2 Zmenu spôsobu autentifikácie zdravotníckeho pracovníka je nevyhnutné premietnuť do legislatívy, čo v súlade s riadnym legislatívnym cyklom je v rozsahu cca 6-7 mesiacov.

Spresnenie identifikovaných rizík: *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Architektúra

Biznis architektúra

Tabuľka 12 Biznis architektúra – budúci stav

Súhrnný popis

Identifikácia a autentifikácia ZPr

Navrhované riešenie eZdravia bude stále podporovať využívanie prihlasovacích kariet ePZP, s tým rozdielom, že karta nebude musieť byť stále zastrčená do čítačky (po autentifikácii je možné ju vybrať).

ePZP aktuálne obsahuje nasledovné certifikáty a zodpovedajúce súkromné kľúče:

X.509 certifikáty

- Autentifikačný certifikát zdravotníckeho pracovníka
- Certifikát pre elektronický podpis zdravotníckeho pracovníka
- Jednorazový šifrovací certifikát zdravotníckeho pracovníka

· RSA súkromné kľúče

- Súkromný kľúč prislúchajúci k autentifikačnému certifikátu
- Jednorazový súkromný kľúč prislúchajúci k šifrovaciemu certifikátu
- Súkromný kľúč prislúchajúci k certifikátu pre elektronický podpis

Funkcionalita, ktorú zabezpečuje autentifikačný certifikát bude nahradená autentifikáciou cez mobilnú aplikáciu a následne aj doplnením funkcionality a metódy do služby „Autentifikačná služba (STS) ZPr“.

Funkcionalita podpisovania a šifrovania, ktorú zabezpečovali zodpovedajúce certifikáty bude riešená pomocou nového centrálneho komponentu nasadeného v NZIS pomocou server signing technológie.

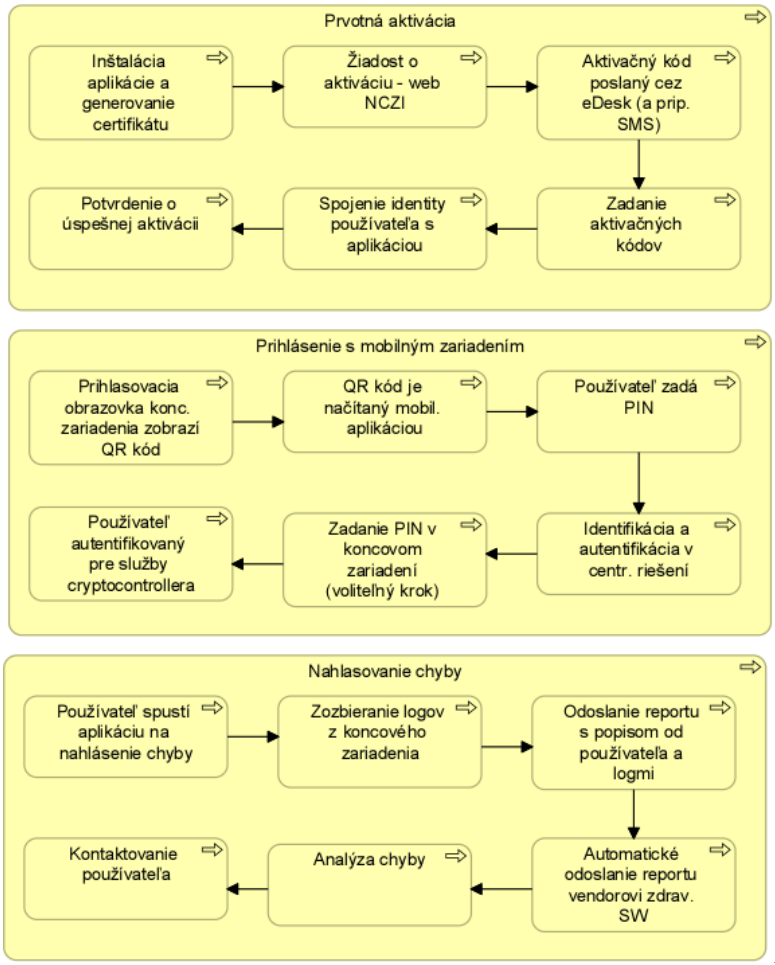
Certifikát	Súčasný stav	Navrhovaný stav bez ePZP
Autentifikačný certifikát	uložený na ePZP	autentifikácia prebehne cez mobilnú aplikáciu
Podpisový certifikát	uložený na ePZP	server signing riešenie
Šifrovací certifikát	uložený na ePZP	server signing riešenie

Z biznis pohľadu zdravotnícky pracovník momentálne na prístup k eZdraviu používa dva faktory – heslo a kartu ePZP. V navrhovanom budúcom stave bude môcť ako druhý faktor okrem karty využívať aj svoje mobilné zariadenie, ktoré bude spárované s centrálnym bezpečným úložiskom v cloude.

Proces registrácie používateľa a mobilného zariadenia bude z používateľského hľadiska nasledovný:

- vloženie ePZP karty do čítačky
- vloženie PIN kódu
- vygenerovanie SAML tokenu (STS server)
- prihlásenie sa na registračný portál (využitie SAML tokenu)
- vytvorenie používateľského konta v bezpečnom centrálnom úložisku
- vygenerovanie certifikátov v bezpečnom centrálnom úložisku
- spárovanie mobilného zariadenia s bezpečným centrálnym úložiskom (používateľským kontom) (využitie mobilnej aplikácie z obchodov aplikácií)

Identifikácia a autentifikácia ZPr bude v rámci eZdravia naďalej zabezpečená aj využitím elektronickej identifikačnej karty (eID). Keďže v eZdraví rola IAM subsystému NZIS pri identifikácii a autentifikácii PrZS spočíva najmä v odtienení aplikačných špecifík v smere k poskytovateľovi identity (IdP-STS) a flexibilnosti takéhoto riešenia, malo by byť možné doplniť ďalšiu metódu autentifikácie prostredníctvom mobilnej aplikácie.



Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Product viewpoint", „Business Process Viewpoint"

Navrhované riešenie subsystému IAM NZIS ma priamy dopad na tieto komponenty z centrálnej a decentralizovaných častí. Centrálnu časť IAM riešenia tvoria nasledovné komponenty:

- infraštruktúra verejných kľúčov,
- autentifikačná služba IAM (STS) pre ZPr,
- systém na správu čipových kariet.

Decentralizovaná časť IAM subsystému navrhované zmeny ovplyvnia najmä v klientskom komponente, ktorý zabezpečuje rozhrania určené na využitie služieb IAM riešenia podporovanými aplikáciami/klientmi IS PZS.

Poznámka: MVSR ako aj NASES momentálne pripravuje projekt alternatívneho autentifikátora. V prípade jeho realizácie by tento projekt mal zabezpečiť potrebné zmeny na strane klientskej časti, aby „Služba potvrdenia prítomnosti a získania identifikátora prijímateľa zdravotnej starostlivosti" fungovala aj s alternatívnym autentifikátorom, t. j. bez použitia fyzickej eID karty.

Monitoring

Bugreporting/monitorovacia aplikácia bude spĺňať nasledovné biznis požiadavky:

- zjednodušenie nasadzovania a aktualizácie centrálynch komponentov potrebných pre fungovanie eZdravia pre lekárov,
- sledovanie stavu koncového zariadenia a možnosť predikcie vzniknutia problému/incidentu,
- možnosť poslať chybové hlásenie, ktoré bude obsahovať relevantné logy a prípadný popis chyby od používateľa,
- možnosť sledovať riešenie chyby a hlasovať o jednotlivých už nahlásených chybách,
- možnosť sledovať štatistiky vlastnej session a celkové štatistiky eZdravia.

Súčasťou navrhovaného riešenia je aj SW a inštancia:

Inštancia KAM, ktorá zjednodušene povedané predstavuje Proxy eZdravie, cez ktoré sa bude pripájať ambulantný ZPr. Inštancia KAM bude obsahovať aj čítačky kariet a čítačky kódov bude teda poskytovať aj služby prístupu na ePZP a eID (t. j. na PC lekára nebude potrebné nič inštalovať),

SW komponent KAM-sw - ktorý predstavuje riešenie pre ambulancie, ktoré si ZPr inštaluje sám na svoj počítač. Tento SW komponent bude riešiť problém súvisiaci s inštaláciou a automatickou aktualizáciou centrálnych komponentov, ktoré si ZPr musí inštalovať.

Potreba nasadenia inštancie KAM alebo KAM-sw riešenia všetkých ambulancií vyplýva z faktu, že v súčasnosti sú centrálne komponenty súčasťou každého ambulantného softvéru, na ktorý NCZI nemá a ani nemôže mať dosah. Rovnako NCZI nemá na úrovni ambulancie monitoring.

KAM inštancia alebo KAM-sw bude povinná pre všetkých ambulantných PZS, povinnosť bude stanovaná v rámci výnosu MZ SR o materiálno-technického vybavenia ambulancií č. 09812/2008-OL.

KAM je určená a zjednoduší prácu v eZdravie pre lekárov a sestry, ktorí majú pracovno-právny vzťah s ambulantným PZS v nasledovných počtoch. Vzhľadom k tomu, že lekári môžu pracovať vo viacerých ambulanciách, celkový počet KAM bol vypočítaný na základe počtu ambulancií a je potrebné ho brať ako maximálny počet v prípade, ak nebude vôbec využité KAM-sw riešenie.

Práve KAM-sw riešenie umožnuje rôzne biznis alternatívy nasadenia riešenia a rovnako umožňuje spôsob objednania inštancie KAM cez rámcovú zmluvu (čo zabezpečí, že inštancie KAM nezostanú nevyužité na sklade).

Povolanie	Počet fyzických osôb
lekár	7 464
zubný lekár	2 564

sestra	9 007

Zaradený len PZS, ktorí prevádzkujú zariadenie ambulantnej zdravotnej starostlivosti a súčasne neprevádzkujú žiadne zariadenie ústavnej zdravotnej starostlivosti

Zdroj: Ročný výkaz M (MZ SR) 1-01 o počte a štruktúre pracovníkov v zdravotníctve, stav k 31.12.2017

V navrhovanom riešení je tiež potrebné rozšíriť a zjednotiť logovanie na strane IS PZS a v prípade potreby tieto logy poskytnúť prevádzkovateľovi eZdravia prostredníctvom navrhovanej bugreportingovej aplikácie.

Kritéria kvality	**Spresnenie kritérií kvality:***Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.*
Výsledok UX testov riešenia *Čas a námaha potrebné na spojazdnenie riešenia* *Čas a námaha potrebné na prihlásenie* *Percentuálny počet nasadených inštancií KAM z požadovaného počtu*	
Riziká	**Spresnenie identifikovaných rizík:***Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
R_3 Neprijatie navrhovaného riešenia zo strany zdravotníckych pracovníkov R_15 Inštancia KAM nebude podporovať všetky požadované konfigurácie	
Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

Architektúra informačných systémov

Tabuľka 13 Architektúra informačných systémov - budúci stav

Navrhované riešenie predstavuje rozvoj ISVS_400, konkrétne časti autentifikácia a monitorovanie. V rámci tejto štúdie uskutočniteľnosti sa analyzovali a navrhovali riešenia pre tieto oblasti:

- vytvorenie systému pre identifikáciu a autentizáciu zdravotného pracovníka prostredníctvom mobilného zariadenia do systému eZdravie

- zabezpečenie inštancií KAM s potrebnou funkcionalitou a úrovňou bezpečnosti,
- vytvorenie systému monitoringu pre KAM a jeho implementácia;

Prihlasovanie

Zvolená alternatíva riešenia spôsobí zmenu v procese identifikácie a autentifikácie ZPr pri komunikácií so systémom NZIS, kde sa celý proces prihlasovania ZPr zefektívni a väčšina procesov sa presunie z koncového zariadenia do centrálneho riešenia. Čítačku kariet a samotnú kartu ZPr nahradí nové riešenie pre mobilné zariadenia ZPr. Nové alebo modifikované komponenty, ktoré budú podporovať samotný proces identifikácie a autentifikácie ZPr sú nasledovné:

- centrálne IAM s API pre komunikáciu s mobilnou aplikáciou,
- server signing riešenie – tzv. centrálny cryptocontroller,
- HSM riešenie pre evidenciu a riadenie životného cyklu certifikátov a zodpovedajúcich privátnych kľúčov,
- logovací modul s nejakým prediktorom, ktorý by sledoval ci je správanie v súlade s definovanými bezpečnostnými pravidlami

- riešenie pre identifikáciu a autentizáciu zdravotného pracovníka prostredníctvom mobilného zariadenia do systému eZdravie

Jednotlivé zmeny z pohľadu architektúry sú popísané nižšie.
IAM subsystém zabezpečí:

- synchronizáciu času medzi IAM a koncovými zariadeniami, ako aj mobilnou aplikáciou, ,
- poskytovanie API na komunikáciu IAM s mobilnou aplikáciou,
- poskytovanie identity prostredníctvom generovania autentifikačných tokenov,
- vygenerovanie PIN kódu pre riešenie pre identifikáciu a autentizáciu zdravotného pracovníka prostredníctvom mobilného zariadenia do systému eZdravie

Funkcionalita centrálneho cryptocontrollera, resp. server signing komponentu bude zabezpečovať všetky funkcie súčasného cryptocontrollera, ale na centrálnej úrovni, t. j.:

- podpisovanie,
- šifrovanie,
- dešifrovanie prijatej komunikácie,
- komunikáciu cez API s koncovým zariadením,
- komunikáciu s HSM.

Technické riešenie autorizácie, t. j. podpisovania s podpisovým certifikátom je navrhované ako server signing riešenie, ktoré funguje na princípe tzv. centralizovaného serverového systému podpisovania. Server Signing riešenie (SSCS – Secure Signature Creation Service) vychádza z požiadaviek normy CEN/TS 419241:2014 – Security Requirements for Trustworthy Systems Supporting Server Signing. Systém by umožnil používateľom generovanie kľúčového páru a následné vydanie certifikátov priamo v centrálnom úložisku. Táto alternatíva predpokladá

vytvorenie riešenia na báze centrálneho bezpečného úložiska kľúčov pre elektronický podpis a funkcionality pre elektronické podpisovanie elektronických dokumentov.

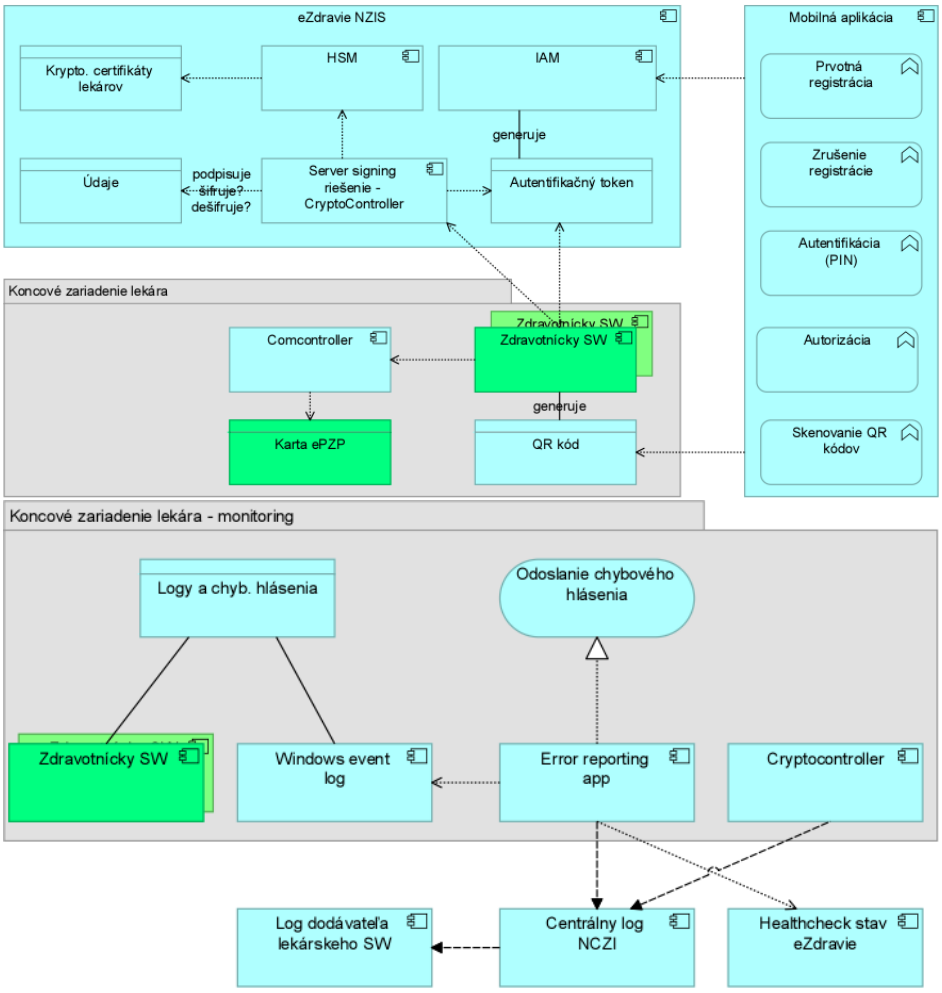
Poznámka: súčasťou riešenia bude aj optimalizácia toku údajov za účelom zrýchlenia komunikácie. T. j. údaje budú tiecť z aplikačných serverov NZIS priamo do cryptocontrollera a až následne do koncového zariadenia (t. j. nie z aplikačných serverov priamo do koncového zariadenia ako to je v súčasnosti).
Funkcionalita komunikácie s kartou ePZP zostane úlohou komponentu Comcontroller, ktorý bude de fakto tvorený torzom súčasného cryptocontrollera. Zabezpečí overenie identity voči IAM pomocou autentifikačného certifikátu uloženého na karte.

Predpokladané **zmeny v zdravotníckom softvéri** sú nasledovné:

- zobrazovanie QR kódu na prihlasovacej obrazovke, a / alebo používanie OTP hesla (na báze OTP protokolu, napr. FreeOTP), konkrétny variant riešenia (aj napr. to, že kde všade má používateľ zadávať PIN, aby to bola vhodná kombinácia bezpečnosti a použiteľnosti by malo vyplynúť z rizikovej analýzy, ktorá bude nedieľnou súčasťou projektu)
- používanie autentifikačného tokenu pri komunikácii s eZdravie,
- zmena API – miesto používania lokálneho cryptocontrollera sa bude používať centrálny cryptocontroller, pričom sa predpokladá použitie REST API,
- revokáciu autentifikačného tokenu v prípade odhlásenia.

Mobilná aplikácia bude poskytovaná na platformách Android a iOS, pričom je ju možné realizovať buď pomocou skenovania QR kódov a autentifikáciou pomocou PIN, alebo ako klasický OTP autentifikátor s tými spojenými možnosťami využitia existujúcich open source implemntácii pre obe platformy.

Autentifikácia všetkých komponentov a dôvera medzi nimi bude na báze autentifikačných tokenov.
Funkcionalita server singing umožňuje aj prehodnotiť potrebu niektorých bezpečnostných funkcií, nakoľko v prípade presunu všetkej funkcionality súčasného cryptocontrollera sa bude na strane servera robiť šifrovanie aj podpisovanie, pričom jeden z týchto úkonov je možný podľa názoru autorov štúdie vypustiť. Prenos údajov z centrálneho cryptocontrollera do koncového zariadenia bude zabezpečený SSL protokolom.

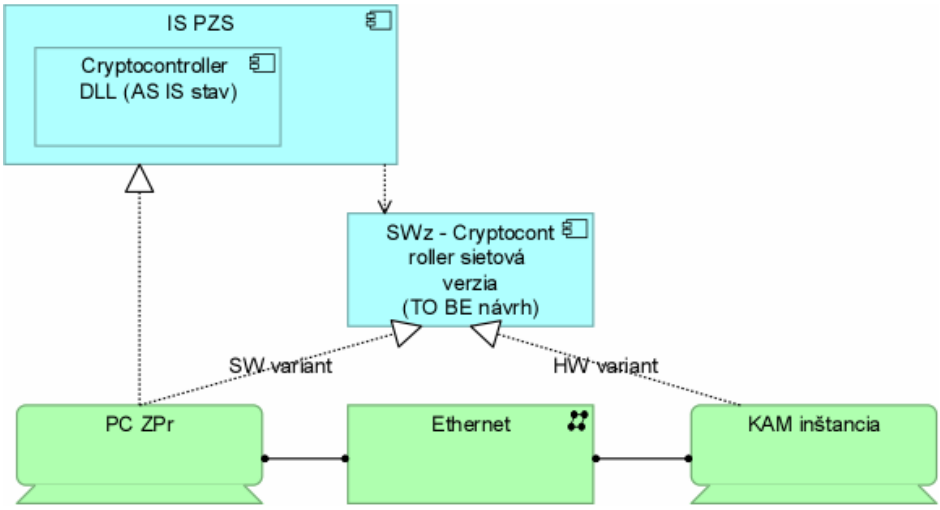


Monitoring

Z aplikačného hľadiska je možné funkcionalitu rozdeliť do dvoch aplikácii (alebo oblastí, keďže sa môžu tváriť ako jedna aplikácia):

- inštalátor NCZI ktorý inštaluje a priebežne aktualizuje cryptocontroller a ovládače čitačiek ePZP/eID
- error reporting a monitorovacia aplikácia – aplikácia na nahlasovanie chýb, ktorá môže byť spúšťaná v prípade požiadavky, resp. chyby, ktorú chce používateľ reportovať. Táto aplikácia bude zabezpečovať:
    - zozbieranie logov z relevantného časového úseku z event logu s možnosťou označenia typu chyby a komentára používateľa,
    - distribúcia chyby do centrálneho logu NCZI (odkiaľ bude následne distribuovaná aj dodávateľovi PZS)
    - možnosť hlasovania o chybách a návrhoch na zlepšenie centrálneho riešenia,
    - zobrazovanie štatistík o aktuálnej session, aktivitách prihláseného lekára, ako aj štatistík eZdravia.

Z hľadiska IS PZS sa jedná o presun funkcionality cryptocontrollera a čitačiek kariet z internej DLL knižnice na úroveň sieťových služieb, ako je znázornené na obrázku nižšie.



Samotná aplikácia, ktorá bude zabezpečovať inštaláciu (na PC ZPr v prípade KAM-sw) a automatické aktualizácie (oba varianty) môže byť rovnaká, vzhľadom na fakt, že obe platformy sú uvažované ako Windows 10 a aj KAM-sw aj inštancia KAM majú poskytovať rovnakú funkcionalitu.

Kritéria kvality

Súčasťou riešenia bude dôkladná riziková analýza na základe ktorej budú realizované konkrétne riešenia

Miera flexibility
Miera použitia štandardných komponentov
Miera použitia štandardných kryptografických funkcií a knižníc

Spresnenie kritérií kvality: *Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.*

Riziká

R_17 Nedostatočné prispôsobenie ostatných častí riešenia eZdravie bude viesť k suboptimálnemu riešeniu

Spresnenie identifikovaných rizík: *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Technologická architektúra

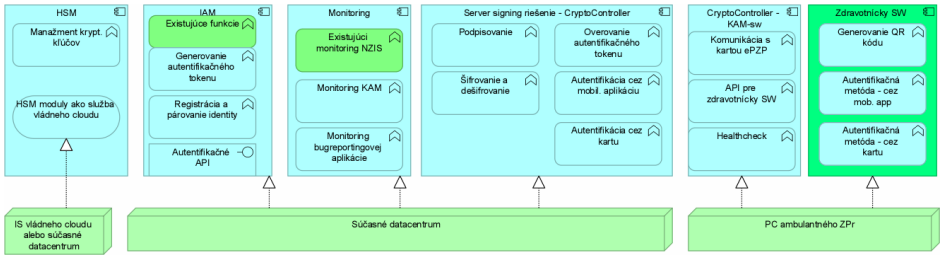
Tabuľka 14 Technologická architektúra - budúci stav

Súhrnný popis

Identifikácia, autentifikácia a autorizácia

Na zabezpečenie požadovaných zmien a funkcií definovaných v biznis a aplikačnej architektúre je potrebné zmeniť, resp. doplniť nasledovné technické komponenty:

- comcontroller, ktorý bude zabezpečovať funkcionalitu ePZP,
- cryptocontroller, ktorý v súčasnosti predstavuje DLL knižnicu, pričom je potrebné, aby bol presunutý do centrálneho NZIS, pričom bude poskytovať podobné služby, ale na centrálnej úrovni a miesto karty bude komunikovať s HSM,
- sieťové HSM, v ktorom budú centrálne uložené certifikáty všetkých používateľov a bude poskytovať služby centrálnemu cryptocontrolleru.
- IAM komponent na poskytovanie identity a generovanie autentifikačných tokenov. Cryptocontroller je komponent implementovaný na strane používateľa. IAM a HSM budú ako centrálne komponenty umiestnené v lokalite, kde je prevádzkovaný aj súčasný NZIS,
- zmeny v IS ZPr,
- samotnú mobilnú aplikáciu pre ZPr, ktorá by realizovala druhý faktor používateľa.



ArchiMate štandardný viewpoint – „Infrastructure Usage Viewpoint", „Infrastructure Viewpoint"

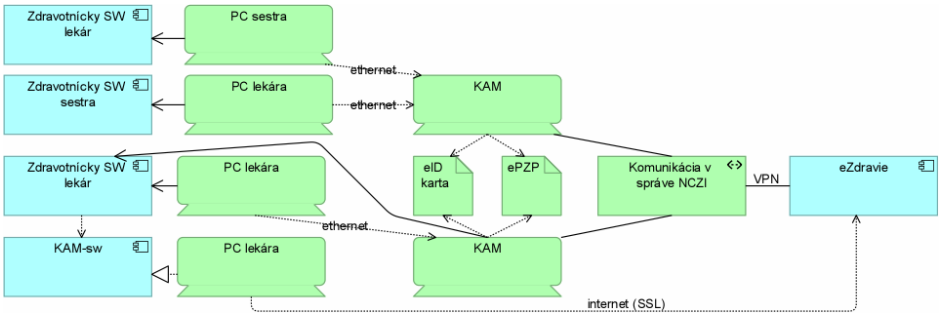
- **Monitoring**

  Z hľadiska technologickej architektúry je potrebné zabezpečiť:
- samotný modul/inštanciu, v prípade inštancie bude doplnený o čítačky ePZP a eID kariet,
- inštanciu s operačným systémom a jeho konfiguráciu tak, aby bola možný vzdialený manažment v doméne NCZI ako aj vzdialená správa,
- organizačno-technické zabezpečenie deploymentu a správy týchto komponentov,
- API pre sieťový prístup k smart kartám a službám e Zdravia aj v offline režime.

  Nasadenie tohto modulu sa predpokladá predovšetkým v ambulanciách v počte max. 25

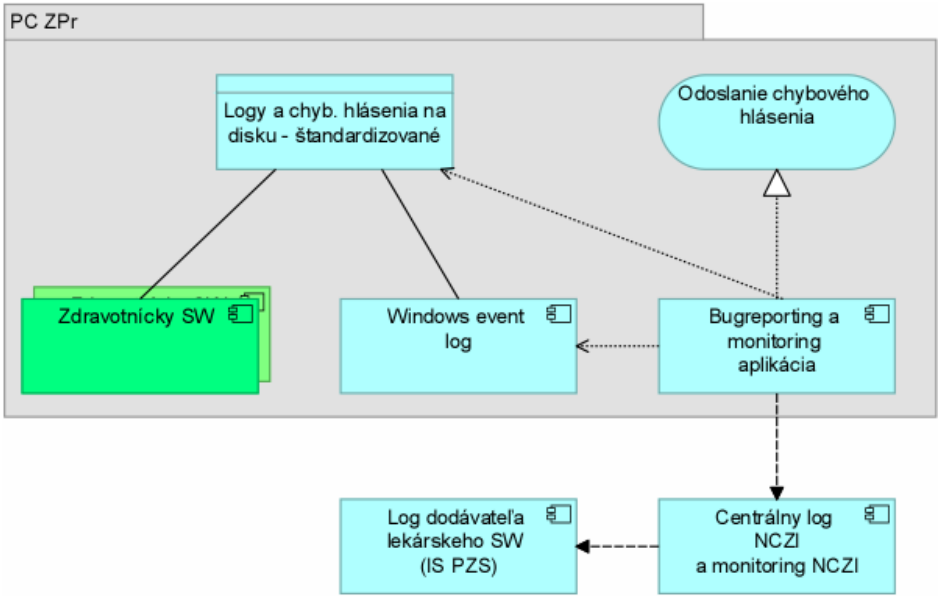
172 kusov (2 ia na ambulanciu, 1 pre sestru a 1 pre lekára, 10 percent je rezerva na reklamácie a chybné kusy). Predpokladané hardvérové požiadavky na zariadenie sú nasledovné:

- podľa možností čo najviac štandardné riešenie,
- kompaktné rozmery,
- sieťové výstupy, aby inštancia mohla byť pripojená k počítaču lekára a mohlo fungovať aj ako router poskytujúci konektivitu do NZIS,
- čítačky pre prístup k smart kartám (ePZP a eID),
- možnosť pripojiť čítačky smart kariet cez USB,
- LTE modem a miesto pre SIM kartu,
- výkonnostné požiadavky, ktoré by mali reflektovať na predpokladanú dobu životnosti 6 rokov.



Obrázok vyššie znázorňuje možné formy pripojenia PC lekára a sestry prostredníctvom KAM k eZdravie. KAM má plní funkciu proxy aj v offline režime a sú k nej pripojené čítačky kariet. KAM prostredníctvom API sprístupňuje služby IS PZS lekára a sestry.

Súčasťou riešenia je aj bugreportingová aplikácia, ktorá slúži na podporu zasielania chybových hlášok pre používateľa. S ohľadom na jednoduchosť inštalácie, aktualizácie a podpory je predpokladaná forma UWP aplikácie publikovanej v Microsoft Store.
Nevyhnutným predpokladom jednotnej aplikácie je definovanie jednotného miesta a spôsobu ukladania chýb a logov zo strany zdravotníckeho softvéru. Predpokladom je kombinácia Windows event logu a úložiska súborov.



Kritéria kvality	**Spresnenie kritérií kvality:***Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.*
Riziká R_16 Integrácia klientskej a serverovej časti	**Spresnenie identifikovaných rizík:***Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
Prílohy *Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.*	**Diagramy, modely, obrázky v plnom rozlíšení** *Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

Implementácia a migrácia

Tabuľka 15 Implementácia a migrácia

Súhrnný popis

Implementácia je predpokladaná v piatich prelínajúcich sa fázach:

Fáza I. – Analýza a dizajn:

- konzultačno-analytické práce spojené s identifikáciou potrebných zdrojov, detailný návrh komponentov a nástrojov, ktoré budú použité v riešení,
- detailná analýza a funkčná špecifikácia, návrh a špecifikácia modulu/inštancie,

- špecifikácia detailných zmien fungovania súčasných centrálnych aplikačných komponentov,
- implementácia a ukážka prototypu riešenia (zároveň spolu s DFŠ).

Fáza II. - Nákup HW a krabicového SW

- Nákup SW licencií a potrebného vybavenia

Fáza III. – Implementácia:

- agilná implementácia a nasadenie v súlade s bežným SDLC (pre neštandardné komponenty),
- priebežné dodávanie funkcionality formou šprintov,
- priebežné školenia.

Fáza IV. – Testovanie:

- testovanie je integrálnou súčasťou každej fázy a každého modulu riešenia,
- v prípade vývoja ide testovanie ruka v ruke s agilným vývojom,
- súčasťou sú obvyklé testovania počas vývoja vrátane testovania interných API, UX testovania mobilnej aplikácie a vytvorenia štandardu login obrazovky pre IS PZS.
- v prípade KAM sa jedná predovšetkým o testovanie potenciálnych integrácii a fungovanie riešenia v prostredí NCZI a eGovernmentu.

Fáza V. – Nasadenie:

- v tejto fáze bude prebiehať deployment KAM do jednotlivých ambulancií, na čo je vyhradený samostatný dodávateľský tím.

Deployment bude prebiehať približne rok a pol, pričom pri počte ambulancií 11 442 vychádza na cca 40 ambulancií denne. Odplata za inštaláciu jedného KAM odhadovaná na 68 eur (t.j. 1,7mil eur celkovo), pričom sa predpokladá, že inštalácia u lekára prebehne v prípade oboch možností, t.j. KAM-sw aj KAM-inštancia. Inštalácia bude považovaná za úspešnú v prípade úspešného zápisu do eZdravia prostredníctvom KAM.

Je potrebné klásť dôraz na:

- podľa možností agilný prístup k vývoju s častým dodávaním prototypov a testovaním (a tvorba DFŠ súbežne s vývojom prototypu/obrazoviek),
- zabezpečenie dostatočného projektového tímu na strane zákazníka minimálne na úrovni garantov, ktorí sa vedia projektu venovať na dennej báze,
- dodržiavanie princípov projektového riadenia PRINCE2 (definované produkty s akceptačnými kritériami, zmenový rozpočet, tolerancie jednotlivých míľnikov, etáp a aj samotných produktov),
- knowledge transfer - transfer vedomostí od dodávateľa členom prevádzkového tímu.

Indikatívny plán VO

Predbežným plánom je realizovať projekt pomocou 3-4 VO, ktoré by mali byť vyhlásené do 4 mesiacov od schválenia štúdie:

- VO na serverovú časť a jej úpravy (server signing),
- VO na aplikačné časti (bugreportin/monitorovacia aplikácia, mobilné aplikácie),
- VO na hardvér, kde sa predpokladá forma rámcovej zmluvy,
- VO na nasadenie KAM u lekárov.

Vecný harmonogram, ktorý zobrazuje rozdelenie na časti a špecifické aktivity projektu je znázornený nižšie. Harmonogram podľa NFP aktivít v súlade s príručkou NFP sa nachádza v tabuľke.

Míľnik	Harmonogram dokončenia od času začiatku v mesiacoch (t – začiatok projektu)
Schválenie štúdie	t-16
Žiadosť o NFP	t-14
Vyhlásenie VO	t-13
Ukončenie VO	t-1
Analýza a dizajn	t+4
Nákup HW a krabicového SW	t+14
Implementácia	t+14
Testovanie	t+14
Nasadenie	t+26

Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Implementation and Migration Viewpoint"

Kritéria kvality Dodržiavanie plánu projektu Funkčné projektové registre a manažment zmien Definované produkty s konkrétnymi a merateľnými kritériami	**Spresnenie kritérií kvality:***Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.*
Riziká R_5 Spolupráca zúčastnených strán nebude dostatočná. Chyby zistené pri testovaní sa nepodarí odstrániť do času uvedenia do prevádzky	**Spresnenie identifikovaných rizík:***Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
Prílohy *Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.*	**Diagramy, modely, obrázky v plnom rozlíšení** *Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

Bezpečnostná architektúra

Tabuľka 16 Bezpečnostná architektúra - budúci stav

Súhrnný popis

Súčasťou bezpečnostnej architektúry sú nasledovné procesy a komponenty:

- prvá aktivácia aplikácie prostredníctvom bezpečných a dôveryhodných kanálov,
- identifikácia koncového zariadenia na ktoré sa používateľ chce prihlásiť,
- identifikácia a autentifikácia používateľa pomocou bezpečného centrálneho úložiska,,
- procesy v ďalšom slede (najmä autorizácia) ostávajú z používateľského hľadiska nezmenené oproti súčasnému riešeniu.

Riešenie sa spolieha na už vybudované riešenie ako aj na centrálne komponenty ako sú eID karta, eDesk schránka, autentifikačný server MVSR.
V rámci tohto projektu je potrebné z pohľadu bezpečnosti zabezpečiť, aby nedošlo k týmto udalostiam:

- impersonifikácia ZPr (predstieranie identity), realizovateľné napr. cez:
    - aktivovanie autentifikačnej aplikácie nesprávnemu používateľovi,
    - kompromitáciu kľúčov CA/HSM,
    - kompromitáciu mobilnej aplikácie,

- kompromitáciu prenosového kanála medzi koncovým zariadením a centrálnym riešením.

V rámci navrhovaného riešenia musí byť zabezpečená:

- Ochrana kryptografických kľúčov certifikačných autorít a komponentov, ktoré majú dosah na impersonifikáciu prostredníctvom kryptografických kľúčov a to samotnou funkcionalitou HSM a faktom, že certifikáty sa nedostanú k používateľom,
- Ochrana prenosového kanála prostredníctvom SSL šifrovania podľa aktuálnych bezpečnostných odporúčaní (napr. forward secrecy a iné) a tým pádom zabezpečenie kanála proti útokom (napr. MITM),
- prevádzka jednotlivých subsystémov v súlade s definovanými organizačnými a bezpečnostnými pravidlami, predovšetkým certifikačnej autority, HSM a dodržiavaním procesu manažment zmien.

Bezpečnostné požiadavky na jednotlivé komponenty riešenia sú nasledovné:
Cryptocontroller:

- na podpisovanie využívať služby centrálneho HSM,
- umožňuje konfigurovať dĺžku session,
- umožňuje vyzvať používateľa na zadanie PIN,

Kľúčové funkcie bezpečnostnej architektúry IAM servera sú najmä:

- správa a riadenie bezpečnostných funkcií,
- bezpečnosť komunikácie s mobilnou aplikáciou a inými komponentami Cryptocontroller a HSM,
- bezpečná sieťová infraštruktúra (routre, firewally, aplikačné firewally)
- generovanie auditných a log záznamov (SIEM - spoločný aj pre Cryptocontroller),
- blokovanie spárovania aplikácie a zariadenia s konkrétnou identitou a rušenie platnosti certifikátov,
- pravidelné kontroly na root, resp. jailbrake mobilného zariadenia zo strany IAM,
- riadenie prístupov,
- bezpečnosť a hardening konfiguračných databáz,
- AV ochrana,
- synchronizácia času,
- bezpečné úložisko kryptografických kľúčov (HSM).

Zároveň si bezpečnosť tohto riešenia vyžiada aj zvýšenie opatrení informačnej bezpečnosti na organizačnej a personálnej úrovni a najmä výkon pravidelných a náhodných bezpečnostných auditov a preverovania logov a prístupov najmä administrátorov a operátorov systému.

Mobilná aplikácia:

- dôsledný sandboxing aplikácie, aby bola zabezpečená jej bezpečnosť,

- Koncové zariadenie a IS PZS
- podporujú zabezpečené spojenie medzi KZ a NZIS, ktoré je odolné voči útokom typu MIDM,

- majú schopnosť použiť autentifikáciu pomocou karty ako aj mobilného zariadenia,
- IS PZS komunikuje s centrálnym cryptocontrollerom,

KAM musí z hľadiska bezpečnosti spĺňať:

- riešenie musí dôveryhodným a optimálnym spôsobom zabezpečovať komunikáciu medzi eZdravie a IS PZS, najmä pomocou použitia štandardných kryptografických funkcií a knižníc (implementácia relevantných častí by mala byť realizovaná v súlade s Common Criteria EAL3)
- riešenie musí obsahovať dôveryhodný spôsob doručovania aktualizácii,
- KAM-inštancia musí byť zabezpečená proti nahradeniu a modifikácii systému.

Súčasťou dodávky riešenia musí byť aj nezávislý bezpečnostný audit treťou stranou.

Z hľadiska monitoringu je pri serverovom riešení potrebné dodržať súčasné bezpečnostné požiadavky, ktoré sú adekvátne. Z pohľadu aplikácie je potrebné dodržiavať analogické relevantné požiadavky ako pri alternatíve ePZP.

Okrem už uvedených požiadaviek je potrebné zohľadniť aj požiadavky na bezpečný a formalizovaný vývoj ako serverovej časti, tak aj klientskej časti a formalizovaný a riadený spôsob kompilácie zo zdrojových kódov. Pri vývoji (kódovaní) sa odporúča aj použitie techník pre „zahmlenie“ (z angl. „obfuscation“) kódu, ktoré sťažujú proces spätného získania kódu z kompilovanej aplikácie (reverse engineering). Nezávislý bezpečnostný audit a prezretie zdrojových kódov je v tomto prípade nevyhnutnosťou.

Kritéria kvality	**Spresnenie kritérií kvality:***Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.*
Akceptovateľný výsledok bezpečnostného auditu vrátane auditu zdrojového kódu mobilných aplikácii a penetračných testov	
Riziká	**Spresnenie identifikovaných rizík:***Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
R_6 Nedodržiavanie organizačných bezpečnostných opatrení a procesov. Riešenie zníži úroveň aktuálnej bezpečnosti	
Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení** *Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	

Prevádzka

Tabuľka 17 Prevádzka - budúci stav

Súhrnný popis

Prevádzkové a bezpečnostné dopady sú determinované predovšetkým požiadavkami existujúceho riešenia. Z pohľadu tohto projektu sa mení iba identifikácia a autentifikácia, ktoré sú definované najmä definovanými bezpečnostnými požiadavkami. Z pohľadu lekára je najvýznamnejšou zmenou forma prístupu k eZdraviu, kedy existujúcu možnosť rozširuje o možnosť prístupu bez karty, ale s pomocou mobilných zariadení. Všetky nové funkcionality, ktoré budú mať priamy dopad na koncových používateľov (ZPr), budú pre používateľa niečo nové a neznáme. Tento fakt môže v úvode používania predstavovať zvýšené nároky na používateľov.
Zvýšené nároky si vyžiada aj prevádzka a udržiavanie integrity, celistvosti a utajenosti centrálneho úložiska certifikátov, ktoré bude zabezpečené technickými, ale aj organizačnými opatreniami. Podobne zvýšené nároky sú na správu systému úložiska certifikátov a transferu certifikátov do cryptocontrollera. V prípade uvoľnenia služieb identifikácie a autentifikácie aj pre tretie strany bude rovnako potrebné pokryť zvýšené nároky na prevádzku systému z dôvodu

zvýšenia jeho komplexnosti, resp. zabezpečenia škálovateľnosti a rozloženia záťaže. Čiastočná minimalizácie tejto zvýšenej záťaže bude kompenzovaná implementáciou monitorovacej aplikácie.
Prevádzka bude zabezpečovať minimálne nasledovné procesy:

- podpora procesu aktivácie/spárovania mobilného zariadenia lekára, vrátane životného cyklu aplikácie,
- správa HSM modulov ako centrálneho úložiska certifikátov používateľov,
- dohľad nad používaním centralizovaných certifikátov a detekcia potenciálnej škodlivej aktivity,
- životný cyklus kľúčov používateľa.

Z hľadiska SLA tieto dopĺňané komponenty tvoria iba malú časť celého systému a po odozvdaní do prevádzky budú prevádzkované pod jeho SLA, t.j.:

- Dostupnosť systému 98%,
- Výpadky – max 175 hodín ročne pričom max 15 hodín mesačne (súčet časov trvania incidentov typu A),
- dĺžka podpory 36 mesiacov + opcia na ďalších 12 mesiacov.

Proces prevádzky KAM

Na základe skúseností NCZI s deploymentov ePZP kariet, ePZP čítačiek a PIN kódov ku kartám, bude správa KAM riešená plne v správe NCZI. NCZI v súčasnosti disponuje tímom 10 zamestnancov na odbore ePZP, ktorí budú plne využití pri podpore KAM. NCZI rovnako disponuje 4 pracovníkmi na oddelení správy aplikácií, ktorí v súčasnosti tvoria výjazdový tím pri riešení incidentu, ktorý vyžaduje zásah priamo v ambulancii lekára.

Niektoré aktivity budú môcť byť outsourcovať na externého dodávateľa, ktorý by zabezpečoval najmä 2nd level HW support,offsite a onsite support.

Zariadenia KAM teda budú v podporované NCZI. Prevádzka KAM nepredpokladá prijímanie nových zamestnancov na NCZI, tím dedikovaný na správu KAM je odhadovaný na 12 zamestnancov.

Prevádzka KAM bude zabezpečovať minimálne nasledovné procesy:

- podpora procesu aktualizácie a deploymentu, vrátane životného cyklu KAM-sw,
- správa KAM-sw a inštancií KAM,
- monitoring KAM, procesy predikcie potenciálnych chýb a riešenie incidentov spojených s KAM,
- dohľad nad používaním systému eZdravie prostredníctvom KAM,
- životný cyklus inštancií KAM.

Kritéria kvality

Zníženie počtu incidentov v pomere k počtu používateľov

Spresnenie kritérií kvality:*Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.*

Riziká

R_7 Nedostatok finančných prostriedkov na pokrytie prevádzky
Neskoré vysúťaženie firmy na podporu a prevádzku HW komponentov
Riešenie bude nákladné na prevádzku

Spresnenie identifikovaných rizík:*Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Ekonomická analýza

Tabuľka 18 Ekonomická analýza - budúci stav

Súhrnný popis

Čistá súčasná ekonomická hodnota (ENPV) =56 961 041 EUR
Rok návratu investície (PBP) =3

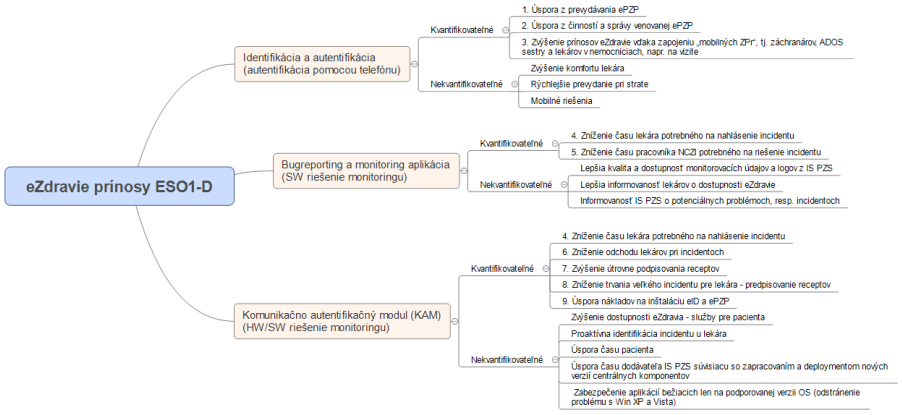
BCR=3.74

Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.

Pri výpočtoch CBA uvažujeme, že v čase spustenia projektu do prevádzky (t.j. cca o 2 roky) bude platit nasledovné:

- väčšina lekárov bude využívať výhody, ktoré systém eZdravie poskytuje a budú sa naňho spoliehať ako na svoj pracovný nástroj
- laboratórne výsledky budú zasielané elektronicky výhradne cez systém eZdravie,
- zdravotnícka dokumentácia pacienta bude zapísaná v eHealth,
- validne budú iba elektronicky podpísané recepty,
- zastúpenie Windows XP medzi lekármi bude 25 percent (aktuálne 37, vypočítané ako odhad budúceho poklesu zastúpenia na základe celosvetového vývoja zastúpenia Windows XP).

Projekt ESO1-D má pomerne veľa technických komponentov, ktoré sú ocenené rôznymi prínosmi. Z dôvodu prehľadnosti uvádzame mapovanie prínosov na jednotlivé časi riešenia. Prínosy sú nasledne popísané nižšie.



Kvantifikovateľné prínosy projektu sú uvedené nižšie. Nekvantifikovateľné prínosy sú uvedené v obrázku vyššie a mali by byť samo-vysvetlujúce.

1. Úspora z prevydávania ePZP

ePZP karta z dôvodov časových obmedzení pri vydávaní certifikátov platí 5 rokov. To znamena, že počas životnosti projektu je potrebné ju 2x prevydať všetkým ZPr. Pri používaní mobilnej autentifikácie však nepotrebujú kartu prevydať všetci ZPr. Uvažujeme, že sa nebude vydávať mobilným ZPr ako aj príslušnému percentu ostatných ZPr, ktorí budú primárne používať mobilnú autentifikaciu.

2. Úspora z činností a správy venovanej ePZP

Správa ePZP je podľa interných údajov NCZI administratívne náročná a nákladná, zahŕňajúca o. i. 11 vyhradených zamestnancov a súvisiace režijné náklady. Nasadenie alternatívnej metódy autentifikácie má potenciál významne znížiť tieto náklady analogicky k penetrácii mobilnej autentifikácie.

3. Zvýšenie prínosov eZdravie vďaka zapojeniu „mobilných ZPr", tj. ZPr pracujúcich pe záchrannú zdravotnú službu

Aktuálne eZdravie nemá riešenie pre mobilných ZPr ako sú záchranári práve z dôvodu, že sa nevedia prihlásiť bez ePZP karty (napr. do mobilnej aplikácie v tablete). V schválenej CBA pôvodného projektu eHealth sú prínosy projektu priamo závislé od počtu lekárov, ktorí system aktívne používajú a predpisujú cez neho lieky. Tieto prínosy aktuálne nie sú materializované. Zapojením mobilných ZPr ako sú práve záchranári však priamo narastá počet lekárov používajúcich system, preto je možné tieto pôvodné prínosy prípisať aktuálnemu projektu.

4. Zníženie času lekára potrebného na nahlásenie incidentu

Na základe štatistík z call centra NCZI bolo vypočítané zdržanie ZPr vyplývajúce z volania a riešenia incidentov. V prípade nasadenia aplikácie by bolo možné nahlasovanie incidentov riešiť automatizovane, pričom predpokladáme, že by sa znížil čas lekára (a opportunity cost aj jeho pacientov) potrebný na nahlásenie incidentu.

5. Zníženie času pracovníka NCZI v call centre

Na základe štatistík z call centra NCZI bolo vypočítané zdržanie ZPr vyplývajúce z volania a riešenia incidentov. V prípade nasadenia aplikácie by bolo možné nahlasovanie incidentov riešiť automatizovane, pričom predpokladáme, že by sa znížil čas pracovníka call centra potrebný na spracovanie týchto incidentov.

6. Zníženie odchodu lekárov pri incidentoch

Počas trvania spomínaného veľkého incidentu bol štatisticky zachytený trend odchodu lekárov zo systému, čo znižuje prínosy eZdravie ako takého. Z historických skúseností je zrejmé, že nasadenie KAM má veľký potenciál tieto odchody znížiť, nakoľko opravy chýb bude možné nasadiť oveľa rýchlejšie.

V období veľkého výpadku (január - marec 2018, 2 incidenty) za 3 mesiace odišlo z eHealth 6,3%, Priemerne sa vrátilo späť 31%. Celkovo teda klesá

používanie eZdravie kvartálne o 4,3%. Nasadenie KAM by tieto incidenty výrazne skrátilo.

Prínos je teda v odvrátení hrozby odchodu týchto lekárov a analogicky ako v prínose č.3 sú lekári ocenení prínosmi z pôvodnej CBA eHealth.

7. Zvýšenie útrovne podpisovania receptov

Elektronický recept je možné zapísať do systému aj bez ePZP karty, je ho však potrebné tlačiť. Tlač si vyžaduje zdržania na strane lekára, recept priemerne 36 sekúnd, ak tlačí jednostranne, 60 sekúnd, ak tlačí obojstranne (priemerne uvažujeme 36 sekúnd, pretože na obojstranné recepty nemamé k dispozícii merania).

V súčasnosti sa pri predpise receptu využíva ePZP iba na úrovni 42%, za posledné reportované obdobie október 2018, bolo podpísaných 1 803 819 a nepodpísaných 2 457 022 elektronických receptov. Po nábehu projektu do prevádzky predpokladáme úroveň 100%.. Ak predpokladáme, že tlač receptu je 36 sekúnd tak benefit je počet receptov x počet minút. Prínos predstavuje odstránenie tohto prestoja pre pacienta a lekára.

8. Zníženie trvania veľkého incidentu pre lekára - predpisovanie receptov

Počas nedostupnosti eZdravia nie je možné elektronicky podpisovať recepty a je nutné ich tlačiť, čo spôsobuje zdržanie pacienta aj lekára. Znížením trvania incidentu je možné tento prestoj odstrániť.

9. Úspora nákladov na inštaláciu eID a ePZP

V prípade preferovaného variantu predpokladáme, že ZPr dostanú inštanciu KAM s predinštalovanými komponentmi potrebnými pre fungovanie eZdravia, čo znamená, že ušetria čas na ich inštaláciu.

Náklady

Náklady na riešenie sa skladajú z nasledovných častí:

- náklady na vývoj serverovej časti riešenia vo výške 0,74 mil eur,
- náklady na vývoj mobilnej aplikácie a monitorovacej/bugreportingovej aplikácie vo výške 0,9 mil. eur,
- náklady na vývoj KAM-sw vo výške 314 tis. eur,
- náklady na nákup inštanciu KAM, čo je plánované ako rámcová zmluva na max. 25 172 kusov (v ambulanciach sú priemerne 2 inštancie, rezerva je uvažovaná 10 percent) za 9,6 mil. eur, pričom nakupovať sa budú iba potrebné kusy,

- náklady na projektové riadenie, publicitu a informovanosť 932 tis. eur,
- vyvolané náklady IS PZS, ktoré sú získané prieskumom u vybraných dodávateľov IS PZS a extrapolované na celú skupinu dodávateľov vo výške 1,7mil. Eur, tieto náklady však nie sú predmetom projektu,
- náklady na deployment KAM, ktoré sú odhadované vo výške 1,7 mil eur (68 eur na KAM).

Porovnanie alternatív

Alternatíva	BCR	ENPV	Rok návratnosti	Poznámka
Alt. A	19,34	33 314 627	2	Finančné ukazovatele nezohľadnujú riziko, že lekári si nebudú vedieť nainštalovať aplikácie vlastnými silami.
Alt. B	3,74	56 961 041	3	Nemonetarizované kvalitatívne prínosy sú oveľa vyššie v prípade alternatívy B, ako vyplýva aj z obrázka vyššie.

Riziká

Spresnenie identifikovaných rizík:*Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

R_ 18 Nepodarí sa dosiahnuť preukázateľné úspory podľa plánu
R_19 Náklady na vybudovanie sa vymknú kontrole/ presiahnu plánovanou hodnotu
R_20 Náklady na prevádzku sa vymknú kontrole/ presiahnu plánovanou hodnotu

Prílohy

CBA projektu