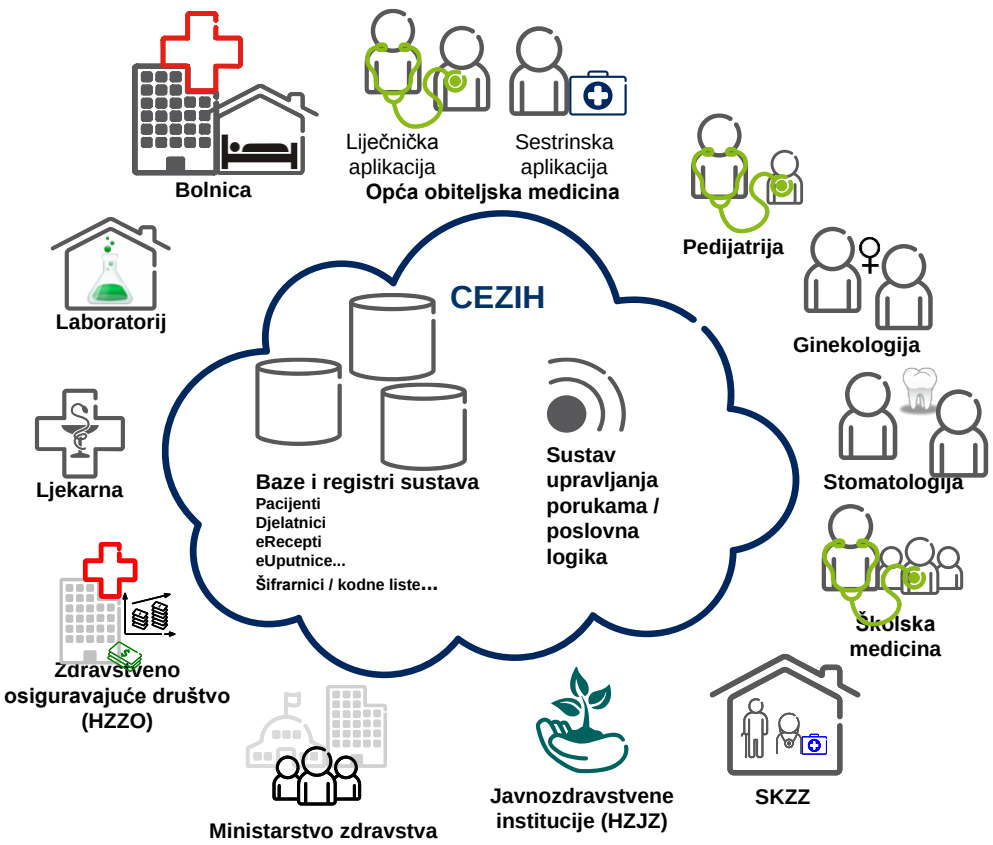
Centralni zdravstveni informacijski sustav Republike Hrvatske (CEZIH) - Koncept sustava

FUNCTION SPEC.



Sadržaj

1 Uvod

1.1 Svrha dokumenta

U dokumentu je dan koncept CEZIH sustava.

1.2 Reference

[1] „Centralni informacijski sustav Republike Hrvatske – Izvješće poslije svakog pregleda (opća obiteljska medicina) – Funkcijska specifikacija“; dok. br. 7/15517-FCPBA 101 24/8 Uhr RevA

[2] „Centralni informacijski sustav Republike Hrvatske – Izvješće poslije svakog pregleda (ginekologija) – Funkcijska specifikacija“; dok. br. 10/15517-FCPBA 101 24/8 Uhr RevA

[3] „Centralni informacijski sustav Republike Hrvatske – Izvješće poslije svakog pregleda (pedijatrija i školska medicina) – Funkcijska specifikacija“; dok. br. 11/15517-FCPBA 101 24/8 Uhr RevA

[4] „Centralni informacijski sustav Republike Hrvatske – Izvješće poslije svakog pregleda (stomatologija) – Funkcijska specifikacija“; dok. br. 12/15517-FCPBA 101 24/8 Uhr RevA

[5] „Centralni informacijski sustav Republike Hrvatske – eRecept – Funkcijska specifikacija“; dok. br. 6/15517-FCPBA 101 24/8 Uhr RevA

[6] „Centralni informacijski sustav Republike Hrvatske – eUputnica (PZZ laboratorij) – Funkcijska specifikacija“; dok. br. 13/15517-FCPBA 101 24/8 Uhr RevA

[7] „Centralni informacijski sustav Republike Hrvatske – eUputnica (izvanbolnički SKZZ) – Funkcijska specifikacija“; dok. br. 14/15517-FCPBA 101 24/8 Uhr RevA

[8] „Centralni informacijski sustav Republike Hrvatske – Izvješće o bolovanju – Funkcijska specifikacija“; dok. br. 15/15517-FCPBA 101 24/8 Uhr RevA

[9] „Prijava maligne neoplazme – Funkcijska specifikacija“; dok.br. 1/15517-FCPBA 101 24/8 Uhr RevA

[10] „Prijava zarazne bolesti – Funkcijska specifikacija“; dok.br. 4/15517-FCPBA 101 24/8 Uhr RevA

[11] „Izvješće o nepoželjnim sporednim pojavama u provedbi imunizacije protiv zaraznih bolesti – Funkcijska specifikacija“; dok.br. 5/15517-FCPBA 101 24/8 Uhr RevA

[12] „Slanje smanjenog Pompidou obrasca – Funkcijska specifikacija“; dok.br. 3/15517-FCPBA 101 24/8 Uhr RevA

[13] „Storno mehanizam – Funkcijska specifikacija“; dok.br. 17/15517-FCPBA 101 24/8 Uhr Rev A

[14] Korisničke upute – helpdesk eRecept;dok.br. 1/00692-FCPBA 101 24/1 Uhr RevC

[15] Korisničke upute – helpdesk eUputnica u PZZ laboratorij;dok. br. 2/00692-FCPBA 101 24/1 Uhr RevC

[16] Korisničke upute – helpdesk eUputnica u izvanbolnički SKZZ; dok. br. 1/00692-FCPBA 101 24/7 Uhr Rev A

[17] „Centralni informacijski sustav Republike Hrvatske – eListe i elektroničko naručivanje u izvanbolnički SKZZ – Funkcijska specifikacija“; dok. br. 16/15517-FCPBA 101 24/8 Uhr RevA

[18] „Centralni informacijski sustav Republike Hrvatske – eNaručivanje – Središnji sustav kalendara vanbolničkog SZKK-a – Korisnički priručnik; dok. br. 4/1553-FCPBA 101 24/8 RevA

[19] „Centralni informacijski sustav Republike Hrvatske – eNaručivanje – Središnji sustav kalendara vanbolničkog SZKK-a – Administratorski priručnik; dok. br. 4/19817-FCPBA 101 24/8 RevA

[20] „Elektroničke smjernice za propisivanje lijekova – Funkcijska specifikacija“; dok.br. 18/15517-FCPBA 101 24/8 Uhr RevA

[21] Arhitektura sustava CEZIH - PZZ grupa:dok.br. 1/12021-FCPBA 101 24/8 Uhr RevC

[22] „Centralni informacijski sustav Republike Hrvatske – Specifikacija kodnih lista“, dok. br. 8/15517-FCPBA 101 24/8 Uhr

[23] „Centralni informacijski sustav Republike Hrvatske – Način korištenja postupaka i slučajeva“, dok. br. 9/15517-FCPBA 101 24/8 Uhr

[24] „Centralni informacijski sustav Republike Hrvatske – Autentikacija korisnika te provjera administrativnih podataka“, dok. br. 19/15517-FCPBA 101 24/8 Uhr RevA

[25] Korisničke upute – aplikacija za upravljanje zamjenama liječnika: dok. br. 3/00692-FCPBA 101 24/7 Uhr RevB

2 CEZIH

2.1 Povijest

Nakon nekoliko neuspješnih pokušaja informatizacije zdravstvenog sustava, napokon je 2002.g. započeo pilot na temelju kojega je na međunarodnom natječaju 2003.g., tvrtka Ericsson Nikola Tesla d.d. (ENT) dobila posao te isporučila središnji dio informacijskog sustava primarne zdravstvene zaštite (stoga se u prošlosti CEZIH označavao i kraticom ISPZZ). Natječaj je bio podijeljen u dvije grupe: G1 i G2 pri čemu je temeljem grupe 1 trebalo isporučiti središnji dio sustava, a temeljem grupe 2 je trebalo isporučiti aplikacije za ordinacije opće obiteljske medicine. Stoga se i danas često za CEZIH može čuti naziv G1, a za liječničke aplikacije opće obiteljske medicine G2. Neformalna nomenklatura je zadržana pa su uvedeni i sljedeći lokalni nazivi:

- G3 – aplikacije za ordinacije za zdravstvenu zaštitu predškolske djece („pedijatrija“)
- G4 – aplikacije za ordinacije za zdravstvenu zaštitu žena („ginekologija“)
- G5 – aplikacije za stomatološku zdravstvenu zaštitu
- G6 – aplikacije za ordinacije za preventivno-odgojne mjere za zdravstvenu zaštitu školske djece i studenata
- G7 – aplikacije za laboratorijsku dijagnostiku (Laboratorijski informacijski sustavi - LIS)
- G8 – aplikacije za ljekarne
- G9 – aplikacije za izvanbolničku specijalističko-konzilijarnu zdravstvenu zaštitu
- G100 – bolnički informacijski sustavi
- G110 – aplikacije za sestrinsku dokumentaciju

Ove aplikacije nisu dio CEZIH sustava, ali zajedno s njim te s još nekim drugim aplikacijama (npr., poslovni sustavi) čine informacijsku podršku poslovnim procesima koji se odvijaju u zdravstvenim institucijama.

CEZIH se kontinuirano razvijao tijekom više od deset godina te održavao sve veći broj usluga od kojih su neke vidljive samo upraviteljima sustava zdravstva i Hrvatskom zavodu za zdravstveno osiguranje, neke i zdravstvenim djelatnicima, a neke i pacijentima.

Jedan od najvećih uspjeha, možda i najpopularnijih usluga CEZIH sustava je elektronički recept (eRecept) čije je puštanje u rad sredinom 2010.g. prva prava nacionalna implementacija elektroničkog propisivanja i izdavanja lijekova u svijetu koja je doživjela nepodijeljene pohvale svih dionika sustava: pacijenata, ljekarnika, liječnika, HZZO-a. Samo mjesec dana kasnije u punu implementaciju je pušten i sustav eUputnice u biokemijski laboratorij čime se u potpunosti informatizirao i ovaj poslovni proces. U pozadini CEZIH nudi još niz usluga koje će biti opisane u nastavku. Svoje prerastanje iz sustava primarne zdravstvene zaštite u Centralni zdravstveni informacijski sustav, CEZIH je krenuo početkom 2011.g. implementacijom elektroničke uputnice u izvanbolničku specijalističko konzilijarnu zdravstvenu zaštitu (SKZZ), a nastavlja ju nadogradnjama koje su najavljene ili su u tijeku poput implementacije elektroničkog upućivanja u bolnice (uključujući otpusno pismo ili nalaz), središnji elektronički zdravstveni zapis, podrška nacionalnim preventivnim programima i sl.

CEZIH je postao vrlo složen informacijski sustav koji se u svojim različitim dijelovima kontinuirano nadograđuje i poboljšava.

Stoga će u ovom dokumentu biti dan pregled sustava te poveznice na dokumente u kojima su opisani detalji o pojedinim dijelovima sustava CEZIH.

2.2 Opća slika

Slika 1. daje pregled sustava CEZIH.

Koncept sustava je takav da klijentske aplikacije razmjenom poruka, a koristeći web servise sustava CEZIH mogu komunicirati međusobno ili prema drugim korisnicima koji imaju pristup podacima unutar sustava. U manjem se opsegu koriste i web aplikacije (helpdesk za eRecept i helpdesk za eUputnicu u PZZ laboratorij, helpdesk za „crvenu“ uputnicu, aplikacija za zamjenskog liječnika[1]), a planiraju se i proširenja u ovom dijelu. S obzirom na relativnu složenost HL7v3 norme, sastavni dio isporuke pa tako i sastavni dio sustava CEZIH za odgovarajuće funkcionalnosti je i tzv., integracijska komponenta (IK). Naime koristeći ovu komponentu, proizvođači klijentskih aplikacija (namijenjena je samostalnim aplikacijama) mogu „zaboraviti“ na složenost HL7v3 norme i kao ulaz u istu u dogovorenom strukturiranom obliku predati samo „korisne“ podatke. Osim samog pretvaranja u HL7v3 poruku, IK komponenta se brije o dostupnosti CEZIH-a (pa tako u slučaju asinkronih poruka i nedostupnosti CEZIH-a iste čuva i isporučuje prvom prigodom), a isto tako se brine o smanjenju opterećenja prema sustavu na način da upite prema CEZIH za preuzimanjem poruka šalje prorijeđeno u slučaju da istih nema u prošlom upitu. IK olakšava i potpisivanje poruka.

[1] Implementacija u tijeku

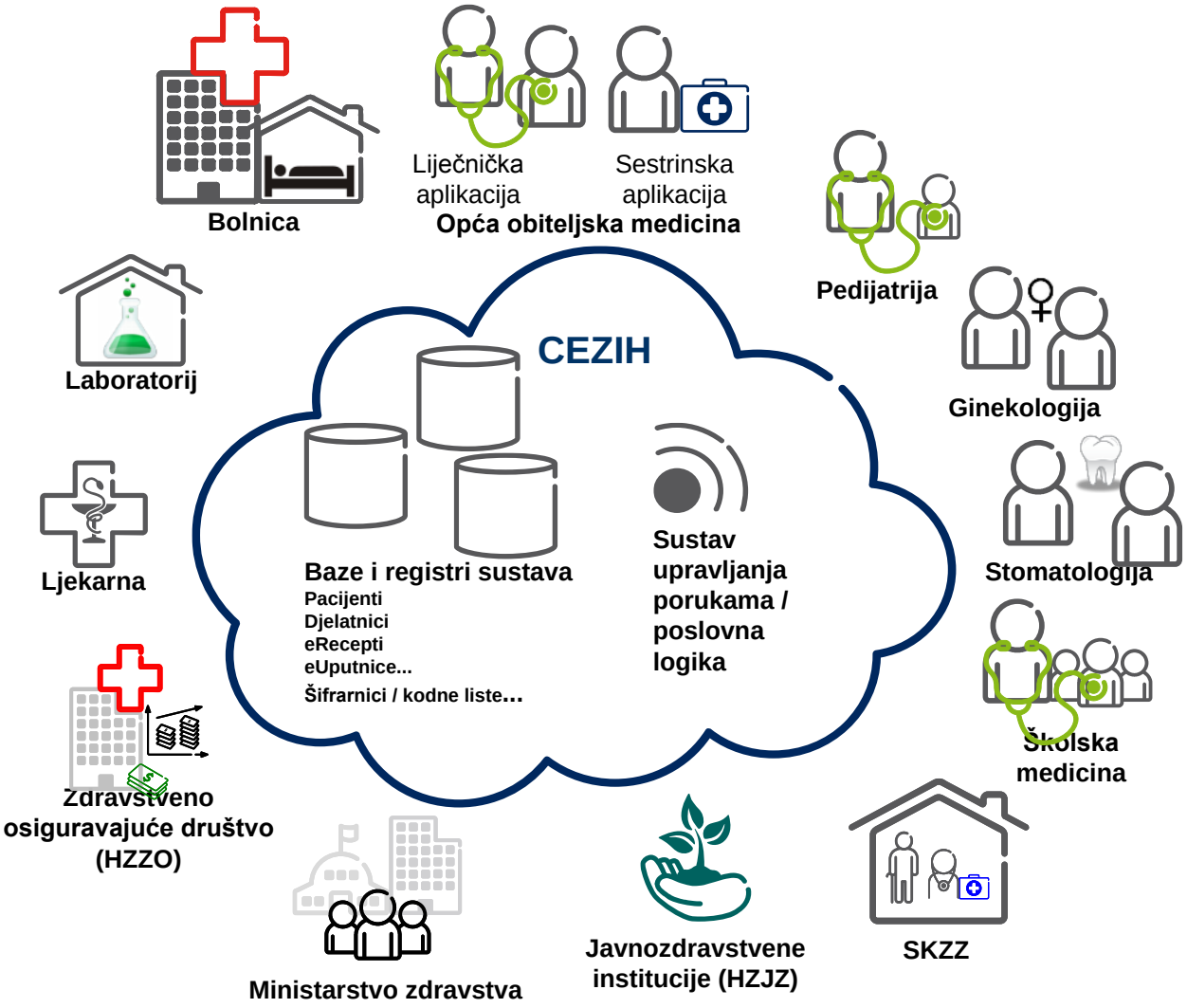
U početku su se koristile isključivo HL7v3 poruke, dok se planiranim nadogradnjama koncept donekle mijenja pa će se za komunikaciju koristiti i HL7v2 poruke odnosno će dio CEZIH sustava postati i dodatne klijentske aplikacije (tako je npr., planirano da središnji elektronički zdravstveni zapis bude web aplikacija kojoj korisnici pristupaju koristeći web preglednik te naravno vlastite pametne kartice za autentikaciju i autorizaciju).

Kako bi se omogućila autentikacija i autorizacija, svakodnevno se iz ZOROH sustava (poslovni sustav HZZOa) automatski u CEZIH baze prebacuju podaci o osiguranim osobama kao i autoriziranim osobama za rad u zdravstvenom sustavu. Ove autorizirane osobe mogu biti zdravstveno i nezdravstveno osoblje, ali se uz svaku osobu prenosi i njegova uloga temeljem koje se daje ili ne daje autorizacija za korištenje odgovarajućih funkcionalnosti CEZIH sustava.

Sve poruke koje korisničke aplikacije razmjenjuju sa CEZIH sustavom moraju biti potpisane digitalnim certifikatom koji se nalazi na pametnim karticama koje korisnicima izdaje HZZO. Nadalje korisničke aplikacije prije početka rada moraju uspostaviti virtualnu privatnu mrežu (VPN) prema CEZIH sustavu.

Za potrebe ispravnog rada različitih mehanizama (poput eRecepta, eUputnice i sl.), iz ZOROH sustava u CEZIH svakodnevno se prebacuju različite kodne liste i šifrarnici (poput liste lijekova). Određeni dio šifrarnika (interno definiranih i potrebnih za rad CEZIH sustava) se administrira lokalno unutar CEZIH sustava, [22].

Dakle dolaskom pacijenta u ordinaciju, liječnik/sestra u lokalnoj G2 aplikaciji registrira dolazak pacijenta. Prije nastavka rada, korisnik kroz lokalnu aplikaciju može provjeriti administrativne podatke pacijenta koristeći web servis na ZOROHu (poslovni sustav HZZO-a) što je primarna varijanta ili to napraviti kroz dvije odvojene poruke prema CEZIH sustavu (koristi se samo u slučaju nedostupnosti HZZO web servisa). Sama implementacija ove provjere (obavlja li se onda automatski prijamom pacijenta, stavljanjem u čekaonicu, ručno ili nešto drugo), ovisi isključivo o implementaciji lokalne G2 aplikacije i nema veze sa CEZIH sustavom te je u pravilu krajnjem korisniku transparentna. Također registracija dolaska je različito implementirana u različitim lokalnim aplikacijama (lokalna čekaonica, izravno otvaranje elektroničke povijesti bolesti…).



Slika 1. Pregled CEZIH sustava

Nakon prijama, liječnik dijagnosticira novi slučaj ili obrađuje postojeći, propisuje recepte i uputnice odnosno obavlja sve aktivnosti potrebne u svrhu pružanja skrbi. Pri tome naravno može koristiti podatke koji o pacijentu već postoje u lokalnoj aplikaciji te naravno upisuje sve potrebne nove podatke (anamneza, status, dijagnoza, status slučaja, uputnica, recept, preporuka liječnika…). Nakon implementacije eKartona, liječnik će dodatne medicinske podatke o pacijentu moći pogledati i koristeći aplikaciju središnjeg elektroničkog zapisa (ovaj će se način vjerojatno češće koristiti u slučaju zamjene liječnika, posjete liječniku izvan vlastitog boravišta i sl. kao i od strane liječnika u bolnicama). Nakon što završi pregled pacijenta i otpusti ga se, lokalna aplikacija od spremljenih podataka formira poruku (izvješće poslije svakog pregleda) koju šalje u CEZIH. Isto tako se ovisno o specifičnom pregledu automatski šalju i dodatne poruke poput Prijave maligne neoplazme ili prijave zarazne bolesti. Ovisno o implementaciji lokalne aplikacije, već tijekom pregleda ili odmah nakon njega, aplikacija šalje i elektroničke recepte, odnosno elektroničke uputnice u biokemijski laboratorij odnosno izvanbolnički SKZZ. S obzirom na zahtjeve poslovnog procesa da pacijent ne smije napustiti ordinaciju dok nije sigurno da je CEZIH preuzeo uputnicu/recept, ove su poruke sinhrone i liječnik u svojoj aplikaciji može vidjeti odgovor od sustava CEZIH te u slučaju da nešto nije u redu, pacijentu izdati papirnate dokumente.

Dolaskom u ljekarnu, ljekarnik na temelju parametara pretrage, dohvaća recepte za pacijenta, po potrebi ih rezervira te šalje podatke o izdanom lijeku i financijskim parametrima izdavanja.

Slično se ponaša i mehanizam uputnice u biokemijski laboratorij, gdje laboratorij može preuzeti uputnicu za pacijenta (kao i eventualnu poruku o uzorku ukoliko je on uzet u ordinaciji), rezervirati je te poslati rezultate natrag u sustav.

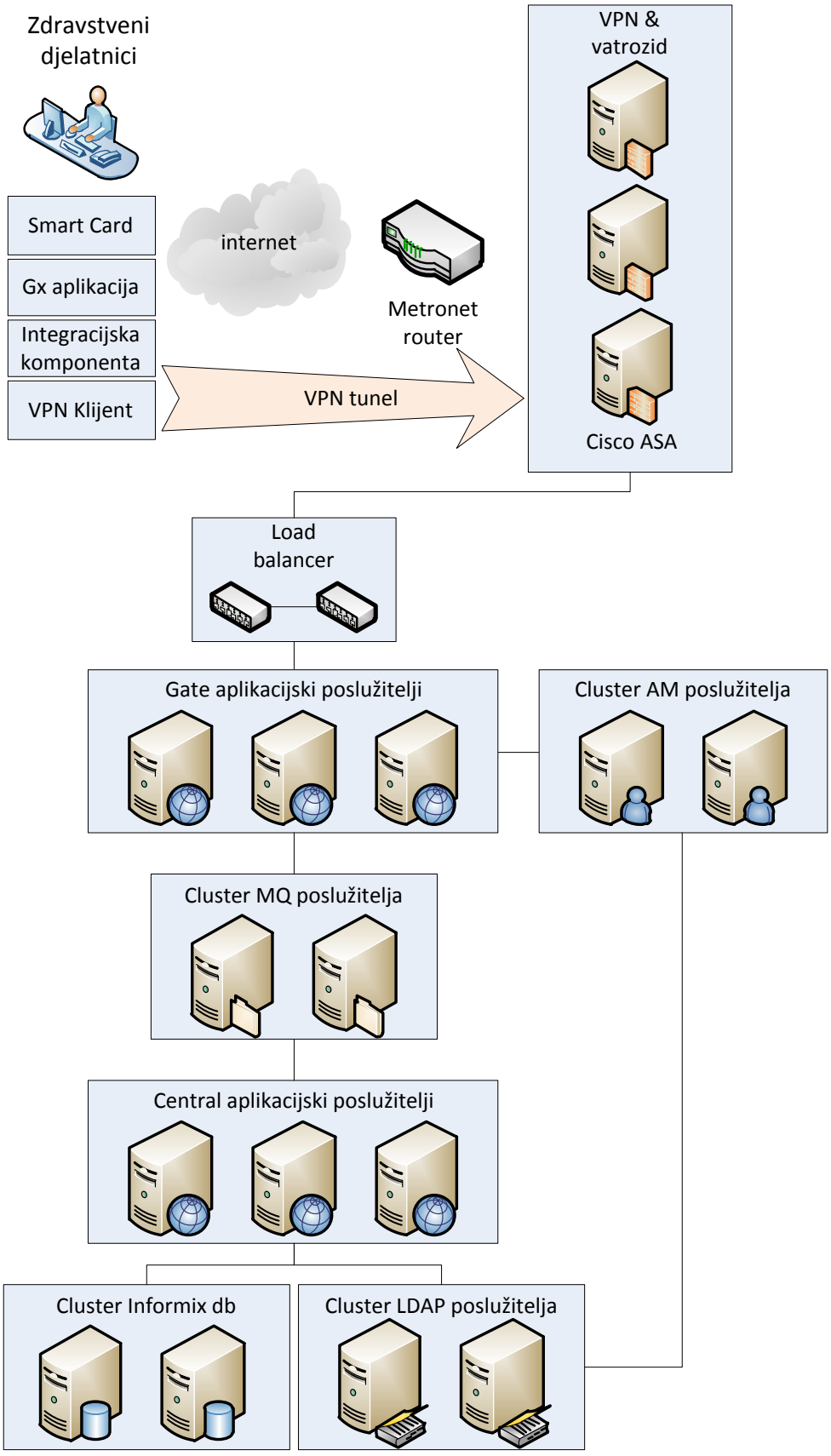
Po dolasku u izvanbolnički SKZZ liječnik specijalist, dohvaća i preuzima uputnicu za pacijenta te šalje nalaze natrag u sustav.

Naravno, CEZIH podržava i sve alternative u ovim procesima (ponovljive recepte, storniranje recepata/uputnica/izvješća, ukidanje ponovljivosti receptu iz izdavanje i bez izdavanja, storniranje nalaza…). Detalji su dani u posebnim dokumentima koji će biti pobrojani u nastavku, dok je način korištenja postupaka i slučajeva obrađen u [23].

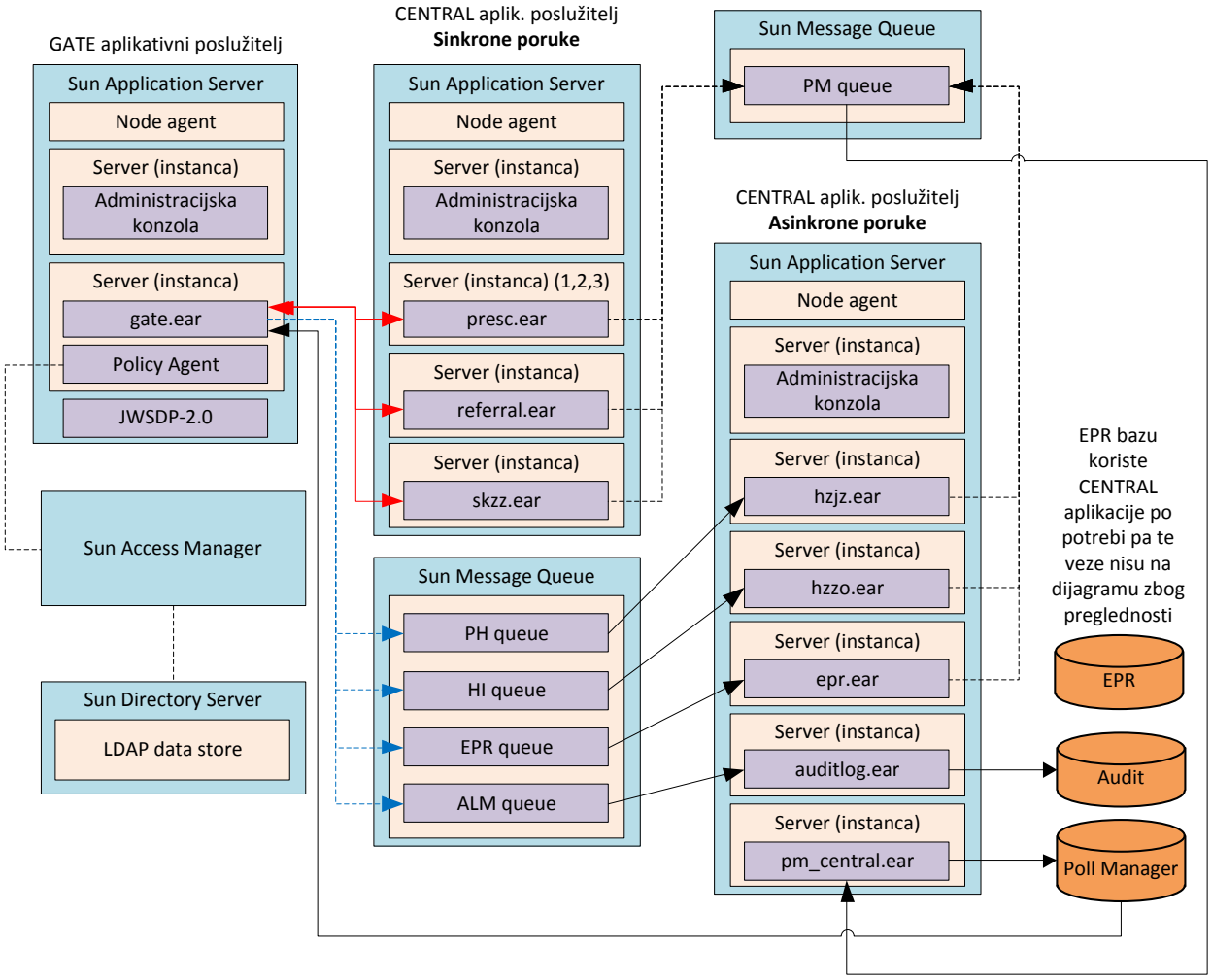
2.3 CEZIH – logička arhitektura

Kako bi se lakše shvatila arhitektura CEZIH sustava u ovom dokumentu su pojednostavljeno prikazane:

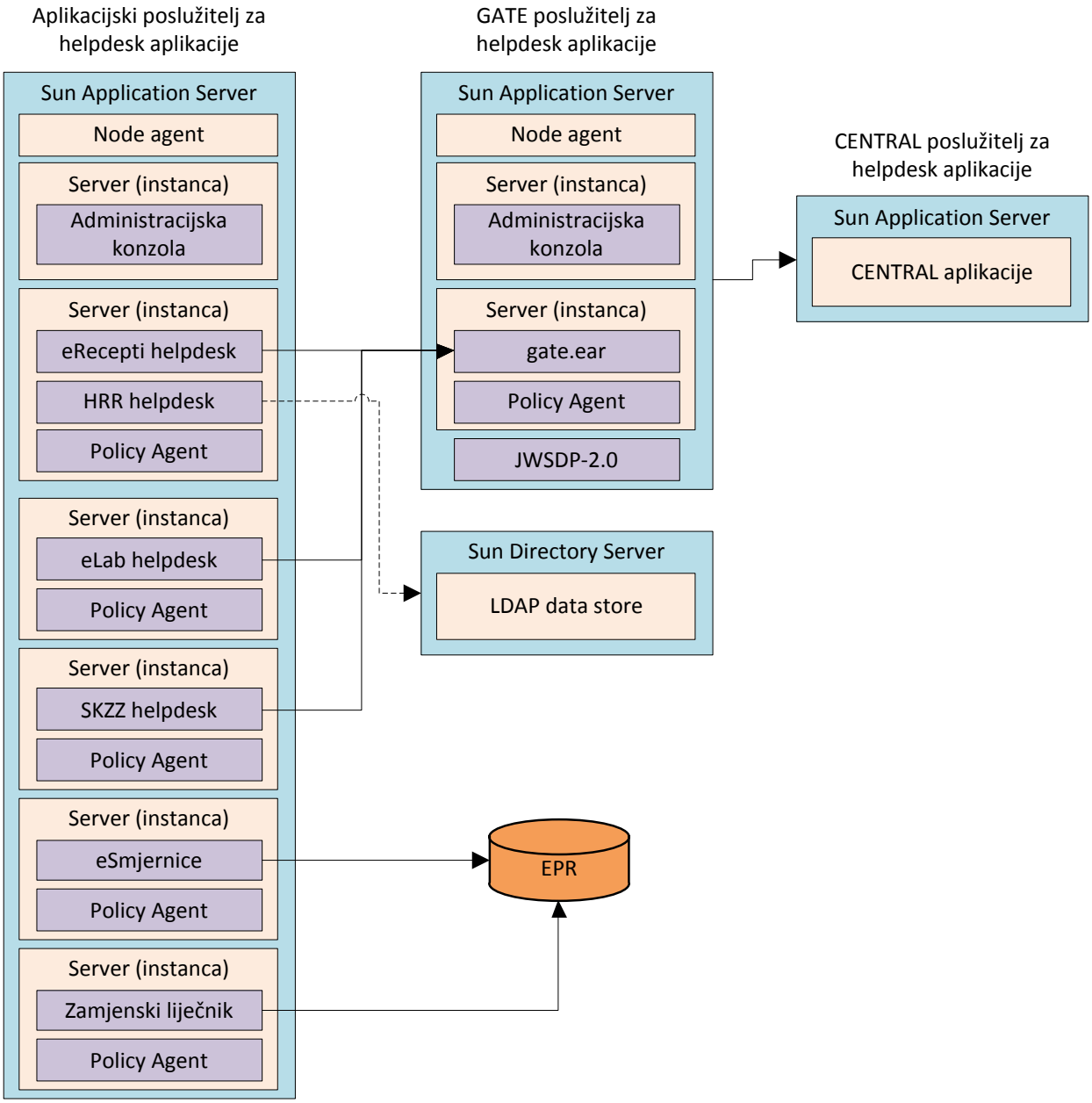
- logičke strukture poslužitelja (tj., kako su povezani poslužitelji) - Slika 2.
- logičke struktura aplikacija (tj., kako su logički povezane aplikacije, rep poruka - MQ i baze) - Slika 3.
- logička struktura za web aplikacije - Slika 4.



Slika 2. Logička struktura poslužitelja



Slika 3. Logička struktura aplikacija



Slika 4. Logička struktura za web aplikacije

2.4 Funkcionalnosti sustava CEZIH

2.4.1 Autentikacija korisnika te dodjela prava korištenja servisa CEZIH sustava

Liječnik na početku radnog vremena otvara svoju aplikacije i treba izvršiti akciju koja zahtjeva interakciju sa CEZIH sustavom te aplikacija radi prvi upit prema CEZIH G1 servisima. Detalji implementacije procesa autentikacije nisu poznati liječniku već su dio unutarnjeg načina funkcioniranja aplikacije koja se spajaju na CEZIH sustav. Kod prvog spajanja aplikacije na CEZIH sustav još nije odrađena autentikacija korisnika te aplikacija prvo treba proći slučaj korištenja „Get Work Permission“ odnosno pozvati servis „Get Work Permission“.

Detaljne specifikacije ove funkcionalnosti dane su u [24].

2.4.2 Provjera administrativnih podataka pacijenta i statusa zdravstvenog osiguranja

Za potrebe provjere administrativnih podataka pacijenta i statusa zdravstvenog osiguranja implementirana su dva servisa koja se koriste u slučaju ako primarna varijanta web servisa na ZOROH-u nije dostupna.

Sama implementacija ove provjere (obavlja li se onda automatski prijamom pacijenta, stavljanjem u čekaonicu, ručno ili nešto drugo, ovisi isključivo o implementaciji lokalne G2 aplikacije i nema veze sa CEZIH sustavom te je u pravilu krajnjem korisniku transparentna).

Detaljna specifikacija ovih funkcionalnosti dana je u [24].

2.4.3 Izvješće poslije svakog pregleda

Ovo funkcionalnost omogućava klijentskim aplikacijama G2-G6 da nakon posjeta pacijenta u ordinaciju primarne zdravstvene zaštite, pošalje sažetak tog posjeta. Poruka se sastoji od podataka i linkova (identifikatora povezanih dokumenata). Naime dio podataka i posjetu je sadržan u samoj poruci (npr., podaci o pacijentu, liječniku, obrađenim slučajevima i sl.), dok je ostatak referenciran identifikatorima ostalih dokumenata/poruka koje su generirane tijekom posjeta (npr., id recepta, id uputnice…). Osim prenošenja različitih podataka radi analize, poruka poslije svakog pregleda će predstavljati osnovu središnjeg elektroničkog zdravstvenog zapisa.

Detaljne specifikacije ove funkcionalnosti za različite specijalnosti unutar primarne zdravstvene zaštite dane su u [1], [2], [3] i [4].

2.4.4 Elektroničko propisivanje i izdavanje lijekova / sanitetskih materijala / magistralnih pripravaka (eRecept)

Ova funkcionalnost omogućava liječnicima da propišu/storniraju recept, a ljekarnicima da dohvate i rezerviraju recept te da pošalju podatke o izdavanju lijeka ili isti ukinu. Osim samog prenošenja podataka te uobičajene validacije atribute, CEZIH obavlja i dodatne provjere na podacima recepta. Detalje ovog mehanizma dan je u [5].

2.4.5 Povezivanje biokemijskih laboratorija

Ova funkcionalnost omogućava liječniku da zatraži odgovarajuće postupke u PZZ laboratoriju za pacijenta (šalje ih elektroničkom uputnicom u CEZIH) te da ukoliko se uzorak uzima u ordinaciji pošalje i podatke o uzorku u CEZIH. Djelatnicima u PZZ laboratoriju je omogućeno da dohvate i rezerviraju uputnicu te pošalju rezultate pretraga natrag u CEZIH odakle ih može dohvatiti liječnik. Detalji o mehanizmu su dani u [6].

2.4.6 Povezivanje ordinacija izvanbolničke specijalističko-konzilijarne zdravstvene zaštite (SKZZ)

Kroz ovaj mehanizam, liječnik može zatražiti određene postupke za pacijenta (šaljući elektroničku uputnicu u CEZIH) od specijalista u izvanbolničkoj specijalistikoj zdravstvenoj zaštiti. Djelatnici SKZZ ordinacija mogu dohvatiti i rezervirati uputnice te poslati elektroničke nalaze natrag u CEZIH odakle ih može dohvatiti liječnik. Detalje o mehanizmu dani su u [7].

2.4.7 Bolovanje

CEZIH kroz ovaj mehanizam omogućuje liječnicima da pošalju u CEZIH relevantne podatke o bolovanju pacijenata. Detalje o mehanizmu dan je u [8].

2.4.8 Prijava maligne neoplazme

U zakonom propisanim slučajevima, liječnik u PZZu je dužan prijaviti slučaj maligne neoplazme što može učiniti slanjem elektroničke poruke u CEZIH. Detalje o mehanizmu dani su u [9].

2.4.9 Prijava zarazne bolesti

U slučaju utvrđivanja jedne od legislativom propisanih zaraznih bolesti, liječnik u PZZu je obvezan prijaviti zaraznu bolest, a dodatno informaciju o tome može poslati u CEZIH. Detalji o mehanizmu su dani u [10].

2.4.10 Izvješće o nepoželjnim sporednim pojavama u provedbi imunizacije protiv zaraznih bolesti

U slučaju da uoči nepoželjne sporedne pojave prigodom provedbe imunizacije protiv zaraznih bolesti, liječnik u PZZu može informaciju o tome poslati elektroničkom porukom u CEZIH. Detalje o mehanizmu dani su u [11].

2.4.11 Smanjeni pompidou obrazac

Prigodom rada s ovisnicima, liječnik u PZZu u legislativom propisanim slučajevima može u CEZIH poslati skup informacija nazvan „smanjeni Pompidou obrazac“. Detalji o mehanizmu dani su u [12].

2.4.12 Storno mehanizam

Pored validacija provedenih u CEZIH sustavu, poslane i isporučene poruke mogu sadržavati netočne informacije. Ovakvi slučajevi se događaju uslijed ljudske pogreške. Takvu je pogrešku nemoguće strojno otkriti te CEZIH posjeduje mehanizam za ispravljanje takvih pogrešaka korisničkom intervencijom. Detalje o mehanizmu daje **Pogreška! Izvor reference nije pronađen.**.

2.4.13 Helpdesk aplikacija za eRecept

Koristeći ovu aplikaciju autorizirani korisnici mogu pristupiti specifičnim informacijama iz eRecept mehanizma kako bi pomogli korisnicima u slučaju potrebe. Detalji o aplikaciji dani su u [14].

2.4.14 Helpdesk aplikacija za eUputnica (u PZZ laboratorij)

Koristeći ovu aplikaciju autorizirani korisnici mogu pristupiti specifičnim informacijama iz eUputnica (u PZZ laboratorij) mehanizma kako bi pomogli korisnicima u slučaju potrebe. Detalji o aplikaciji dani su u [15].

2.4.15 Helpdesk aplikacija za eUputnicu (u izvanbolnički SKZZ)

Koristeći ovu aplikaciju autorizirani korisnici mogu pristupiti specifičnim informacijama iz eUputnica (u izvanbolnički SKZZ) mehanizma kako bi pomogli korisnicima u slučaju potrebe. Detalji o aplikaciji dani su u [16].

2.4.16 Elektroničko naručivanje u izvanbolnički SKZZ

Ova funkcionalnost omogućava liječnicima iz PZZa da naruče pacijenta na odgovarajući postupak u ordinacije izvanbolničkog SKZZ. Detalji su opisani u [17][17]. Dodatna dokumentacija je dana u dva priručnika:

- Korisnički priručnik [18] te

- Administratorski priručnik [19][19].

2.4.17 Elektroničke smjernice za propisivanje lijekova

Ova funkcionalnost olakšava propisivanje lijekova sukladno odgovarajućim smjernicama. Detalji su opisani u [20].

2.4.18 Aplikacija za upravljanje zamjenama liječnika

Funkcionalnost aplikacije za upravljanje zamjenama liječnika omogućava trima korisničkim ulogama administriranje članova liječničkih timova. Prava u aplikaciji su definirana korisničkom ulogom koju korisnik aplikacije ima. U aplikaciji su definirane tri uloge s pripadajućim pravima administracije:

- liječnik (nositelj tima) - prava administracije vlastitog tima
- ovlaštena osoba u domu zdravlja- administracija timova unutar doma zdravlja
- djelatnik HZZO helpdesk-a za sve timove

Detalji su opisani u [25].

2.5 Arhitektura

CEZIH je u desetak godina svog postojanja postao poslovno kritičan sustav za zdravstveni sustav odnosno njegove dionike. U tom smislu arhitektura CEZIH sustava se kontinuirano prilagođava potrebama, a trenutno stanje opisuje dokument [21].

3 Sigurnosni aspekti sustava CEZIH

3.1 Uvod

Arhitektura CEZIH rješenja u skladu je s osnovama informacijske sigurnosti i to:

- Povjerljivosti
- Integritetom
- Dostupnošću

S obzirom na osjetljivost podatka, CEZIH rješenje primjenjuje visoke standarde vezane uz implementaciju sigurnosti. Osnovni zahtjevi vezani uz CEZIH rješenje su:

- povjerljivosti podataka
- kontrola pristupa
- visoka dostupnost
- višeslojna implementacija rješenja.

Arhitekturu CEZIH sustava možemo podijeliti u dva dijela uzimajući u obzir načine pristupa odnosno sučelja. Sučelje prvog tipa je realizirano preko web servisa na koje se spajaju klijentske aplikacije uglavnom koristeći IK komponentu. Funkcionalnosti obuhvaćene tim sučeljem su navedene u poglavljima od 2.4.3 do 2.4.11. Drugi tip su web aplikacije koji korisnici direktno koriste kroz web preglednike. To su funkcionalnosti iz poglavlja 2.4.13 do 2.4.16.

Sigurnosne značajke CEZIH sustava možemo dva segmenta. Prvi segment obuhvaća zajedničke infrastrukturne i arhitekturalne značajke dok drugi segment obuhvaća aplikativne značajke u ovisnosti o realizaciji samih aplikacija.

3.2 Arhitekturalne značajke

3.2.1 Infrastruktura

3.2.1.1 Virtualna Privatna Mreža (VPN)

CEZIH sustav odvojen je od ostatka Internet mreže VPN-om. To znači da je onemogućen pristup do CEZIH servera bez ostvarivanja VPN tunela. Ovo vrijedi za svaku funkcionalnost CEZIH sustava. VPN se realizira na CEZIH VPN serverima. VPN serveri prilikom ostvarivanja VPN veze zahtijevaju klijentski certifikat. Klijentski certifikati izdani su na *smart* karticu korisnika. VPN serveri prihvaćaju samo validne certifikate izdane od strane CEZIH certifikacijskog tijela. VPN veze se ostvaruju od svakog klijenta po principu udaljenog pristupa (*eng. remote access*).

Ukoliko se ne uspostavi veza naknadno nije moguće spajanje na CEZIH sustav. U tom slučaju klijentske aplikacije ipak mogu nastaviti s radom o *offline* modu.

3.2.1.2 Vatrozid

CEZIH infrastruktura obuhvaća i vatrozide kojima se razdvajaju CEZIH serveri te definiraju pristupni protokoli i portovi.

Vatrozidom je krajnjim korisnicima omogućen pristup samo preko https veze na definiranim pristupnim adresama i portovima. Direktan pristup serverima od strane krajnjih korisnika nije moguć.

3.2.1.3 Balansiranje prometa

Sav promet koji se upućuje od strane korisnika propušta se kroz balansere prometa (*eng. load balancer*). Za servisno sučelje promet se balansira između niza servera na web sloju (gate serveri). Isto tako svaka od web aplikacija instalirana je na barem dva servera. Veza se ostvaruje preko jedne adrese nakon koje se promet balansira prema oba servera. Time se postiže visoka raspoloživost sustava te uravnoteženje opterećenja.

3.2.2 Povjerljivost

Povjerljivost podataka osigurava se šifriranjem transportnog kanala pomoću Secure Socket Layer/Transport Layer Security (SSL/TLS) sloja. Sva komunikacija između korisnika CEZIH sustava bilo preko web aplikacije ili web servisa je šifrirana. Šifrirana je i komunikacija između CEZIH web aplikacija i CEZIH web servisa. Krajnjim korisnicima otvoreni su samo https portovi. Korisnici nemaju mogućnost pristupa aplikaciji niti na koji način preko standardnog http porta.

Uz enkripciju kanala, pomoću SSL/TLS mehanizma potvrđuje se i autentičnost servera na koji se spajaju klijenti. Klijenti mogu biti sigurni da server na koji se spajaju zaista pripada CEZIH rješenju. U tu svrhu svi klijenti moraju imati instaliran ishodišni certifikat CEZIH CA certifikacijskog tijela.

SSL/TLS komunikacija realizirana je na aplikativnim serverima na web sloju CEZIH sustava.

3.2.3 Upravljanje ključevima

Unutar CEZIH rješenja koristi se pet tipova certifikata. Svi certifikati izdaju se od CEZIH certifikacijskog tijela. Certifikate možemo podijeliti s obzirom na namjenu za koju se koriste.

Prvi tip certifikata je serverski certifikat koji se koristi za uspostavu sigurnog transportnog kanala (SSL/TLS). Ovaj certifikat se nalazi u obliku zaštićene datoteke na CEZIH strojevima u web sloju.

Drugi tip certifikata su aplikativni certifikati. Oni se izdaju web aplikacijama koje se spajaju na CEZIH web servise. Služe za prijavu web aplikacija kao klijentski certifikati. Nalaze se u obliku zaštićene datoteke na serverima web aplikacija.

Treći tip certifikata je certifikat izdan centralnom CEZIH sustavu. Koristi se za potpisivanje odlaznih poruka iz G1 sustava. Nalazi se u obliku zaštićene datoteke na svim centralnim serverima G1 sustava.

Četvrti tip certifikata je potpisni certifikat. CEZIH sustavu je izdan potpisni certifikat koji se koristi u svrhu potpisivanja koda. Tim certifikatom potpisan je sav kod koji se izvršava na strani korisnika kroz Internet preglednike.

Peti tip su klijentski certifikat izdani krajnjim korisnicima (zdravstvenim djelatnicima). Klijentski certifikati izdaju se zdravstvenim djelatnicima na pametne kartice (eng. s*mart cards*). Klijentski certifikati koriste se za prijavu na CEZIH rješenja te za potpisivanje poruka koje se razmjenjuju preko web servisa.

3.2.4 Administracija korisnika

Administraciju korisnika usluga i dodjelu ovlasti provodi HZZO.

HZZO djelatnici (po područnim uredima) korištenjem ZOROH funkcije dodjeljuju ovlasti zdravstvenim djelatnicima. Kroz ZOROH aplikaciju se također pokreću procesi izrade i dostave pametnih kartica.

Za zdravstvene djelatnike koji imaju pravo na korištenje neke od usluga u sustavu CEZIH, HZZO sustav do CEZIH sustava dostavlja podatke (u ldif formatu) za ubacivanje u HRR imenički servis. Ti podaci sadrže identifikacijske podatke korisnika kao i popis ovlasti (uloge). Sve CEZIH usluge koriste HRR imenički servis kao osnovni korak sigurnosne provjere ovlasti.

Pojedine aplikacije (npr., dostup do sadržaja populacijskog registra) zahtijevaju dodatne podatke - vezu odabranog liječnika i pacijenta te pripadnost timu odabranog liječnika. Podatke o odabranim liječnicima i članovima tima administrira HZZO u eprd_a bazi podataka CEZIH sustava.

3.2.5 Revizija (eng. *audit*)

Svi bitni detalji vezani uz korištenje CEZIH sustava se zapisuju.

Prilikom prijave na sustav zapisuju se uspješni i neuspješni slučajevi na nivou servera za kontrolu pristupa.

Zapisi o pristupu bilježe se u logove na nivou svih pristupnih servera. Greške se također zapisuju na nivou svih CEZIH servera.

Navedeni zapisi vrijede za oba tipa sučelja: web servise i web aplikacije.

Dodatno treba napomenuti da se sve ulazne poruke na servisnom sučelju bilježe u bazu. Na taj način mogu se analizirati poruke i utvrditi potpisnici pojedinih poruka te poslanih podatka.

3.3 Aplikativne značajke

3.3.1 Web servisi

3.3.1.1 Prijava

Korisnici klijentskih aplikacija šalju poruka na centralni sustav kojom se provjerava dozvola za rad korisnika odnosno pošiljatelja (*Get Work Permission).*

Prilikom slanja poruke *Get Work Permission* aplikacija ostvaruje konekciju prema aplikativnim serverima CEZIH sustava. Kao što je već spomenuto veza između pošiljatelja i aplikativnih servera na CEZIH strani je šifrirana uspostavom SSL/TLS kanala.

Prilikom uspostave SSL/TLS od strane CEZIH sustava zahtjeva se autentikacija preko klijentskog certifikata. U tu svrhu se koristi djelatnikov certifikat na pametnoj kartici. Djelatnikov certifikat mora biti izdan od strane CEZIH certifikacijskog tijela te mora biti valjan. Isto tako mora postojati djelatnikov korisnički zapis u imeničkom servisu korisnika na CEZIH sustavu. Usporedba certifikata i korisničkog zapisa vrši se preko jedinstvenog matičnog broja (MBO) pohranjenog u samom certifikatu te u imeničkom servisu korisnika. Ukoliko bar jedan od ovih uvjeta nije ispunjen prijava neće biti uspješna, odnosno pošiljatelj neće dobiti dozvolu za rad sa CEZIH sustavom. Uspješni i neuspješni pokušaji autentikacije se zapisuju na serverima CEZIH sustava.

Klijentske aplikacije (Gx) uglavnom koriste Integracijsku komponentu za formiranje poruke i uspostavu komunikacije prema CEZIH sustavu.

Jednom kad je ostvarena prijava na sustav dalje se ostale poruke preko servisnog sučelja šalju kroz istu korisničku sesiju.

3.3.1.2 Autorizacija

CEZIH autorizira korisnika odnosno provjerava da li korisnik ima pravo slati poruku u CEZIH sustav. Autorizacija unutar CEZIH sustava se vrši na principu uloga. Svaki korisnik u imeničkom servisu korisnika CEZIH sustava ima pridijeljene uloge. Ukoliko korisnik posjeduje ulogu koja je definirana za specifičnu poruku, slanje je dozvoljeno. Ukoliko korisnik nema niti jednu od dozvoljenih uloga slanje poruke se odbija. U dokumentu [5] se primjerice definiraju prava pristupa za poruke u eRecept mehanizmu (analogno vrijedi za eUputnica u PZZ laboratorij i eUputnica u izvanbolnički SKZZ). Uspješno slanje poruka kao i odbijanje poruke se zapisuje u logovima aplikacijskih servera na CEZIH sustavu.

Autorizacija na CEZIH sustavu je podešena tako da je dozvoljeno slanje poruke *Get Work Permission* svim autenticiranim korisnicima

3.3.1.3 Neporecivost

Zahtjev od strane CEZIH sustava je da sve poruke koje budu upućene prema centralnom sustavu budu potpisane. S obzirom na osjetljivost podatka potrebno je osigurati povjerljivost i integritet na nivou poruke. Uz ova dva sigurnosna aspekta potpisom se direktno osigurava i neporecivost na nivou same poruke. To znači da svaki klijent CEZIH sustava svojim potpisom direktno i neporecivo povezuje svoj identitet sa podacima koji se zapisuju u poruku.

Komunikacija prema CEZIH sustavu realizirana je preko web servisa koristeći Simple Object Access Protocol (SOAP) protokol koji je baziran na eXtensible Markup Language (XML). Potpis XML poruke realiziran je u skladu s W3C XML Signature Syntax and Processing specifikacijom (XML DSig). Tip XML DSig potpisa je *detached signature*.

Poruka se potpisuje prije slanja od strane klijentske aplikacije pomoću klijentskog certifikata na pametnoj kartici. Prilikom provjere potpisa na CEZIH strani provjerava se valjanost certifikata te integritet podataka odnosno valjanost potpisa. Ukoliko barem jedan od ovih uvjeta nije ispunjen poruka se odbija te CEZIH sustav šalje povratnu informaciju o grešci.

Poruke koje dolaze do klijentskih aplikacija od strane CEZIH sustava su također potpisane od strane CEZIH sustava. Za tu namjenu izdan je aplikativni certifikat od strane CEZIH certifikacijskog tijela. Taj certifikat predstavlja identitet CEZIH sustava. Valjan potpis i certifikat garantiraju integritet samih podataka pristiglih do klijentskih aplikacije te identitet kreatora odnosno potpisnika poruke, u ovom slučaju CEZIH sustava.

Sve poruke koje ulaze u CEZIH sustav se pohranjuju. Naknadnim pretraživanjem može se utvrditi koji su podaci ušli u CEZIH sustav te tko ih je kreirao odnosno potpisao.

3.3.1.4 Validacija ulaznih podataka

Podaci unutar poruka koje se šalju preko servisnog sučelja se semantički provjeravaju. Validacija obuhvaća provjeru valjanosti poslanih podataka odnosno tip, format, vrijednost i slično. Ukoliko provjera nije uspješno prošla vraća se poruka o grešci. Detalji semantičke provjere unutar primjerice eRecept mehanizma opisani su u dokumentu [5].

3.3.2 Web aplikacije

3.3.2.1 Prijava

Prijava na web aplikacije odvija se prilikom spajanja na aplikaciju. Svaka aplikacija zahtijeva prijavu putem korisničkog certifikata. Koriste se certifikati s pametnih kartica izdanih od strane CEZIH certifikacijskog tijela. Kao i za servisni dio mora postojati djelatnikov korisnički zapis u imeničkom servisu korisnika na CEZIH sustavu. Usporedba certifikata i korisničkog zapisa vrši se preko jedinstvenog matičnog broja (MBO) pohranjenog u samom certifikatu te u imeničkom servisu korisnika. Imenički servis te server za kontrolu pristupa zajednički su servisnom sučelju i web aplikacijama.

3.3.2.2 Autorizacija

Autorizacija pristupa web aplikacijama vrši se također na osnovu ovlasti odnosno uloga koje su pridijeljene korisnicima. Kontrola pristupa realizirana je na serverima za kontrolu pristupa te uz konfiguraciju samih aplikacija.

Helpdesk aplikacije namijenjene su helpdesk korisnicima te omogućavaju pristup samo korisnicima s helpdesk ulogama. Autorizacija za helpdesk aplikacije je realizirana tako da nema granulacije funkcionalnosti po ulogama, ukoliko korisnik ima ovlasti za rad s aplikacijom može koristiti sve funkcionalnosti aplikacije.

Aplikacija zamjenskog liječnika[2] će biti posebna u tom smislu što je koriste i helpdesk djelatnici i liječnici. Na nivou aplikacije postoje funkcionalnosti namijenjene pojedinim ulogama.

3.3.2.3 Komunikacija sa centralnim sustavom

Helpdesk aplikacije sadržavaju određene funkcionalnosti koje zahtijevaju komunikaciju sa G1 servisnim sučeljem.

U tim slučajevima helpdesk aplikacije se ponašaju kao klijentske aplikacije G1 sustav. Prilikom spajanja koristi se aplikativni certifikat izdan helpdesk aplikacijama. Potpis poruka vrši se koristeći korisnikov klijentski certifikat na pametnoj kartici pomoću *appleta* koji se izvršava na korisničkom računalu.

3.3.2.4 Validacija ulaznih podataka

Pri izradi web aplikacija vodilo se računa o kontroli unosa podataka. Ulazni podaci se validiraju. Polja za unos podataka kontroliraju tip i veličinu podatka omogućavajući korisniku unos samo valjanih podatka. Nadalje implementirane su kontrole valjanosti podataka pri samom unosu javljajući npr., korisniku grešku prilikom unosa određene šifre.

[2] Implementacija u tijeku

3.3.2.5 Potpisivanje koda

Neke od web aplikacije sadrže kod koji se izvršava na korisničkoj strani (eng. *applet*). Kod koji se izvršava na korisničkoj strani potpisuje se certifikatom koji je izdan od strane CEZIH certifikacijskog tijela. Prije instaliranja nove verzije takvih aplikacija svaki put se iznova potpisuje kod istim certifikatom.

Klijenti koji koriste web aplikacije s potpisanim kodom moraju vjerovati certifikatu kojim se potpisuje kod. Na taj način klijenti mogu biti sigurni da na svom računalu izvršavaju provjeren i potvrđen kod. U tu svrhu klijenti trebaju instalirati ishodišni CA certifikat CEZIH certifikacijskog tijela. Uz njega treba instalirati i javni dio potpisnog certifikata. Oba certifikata treba instalirati u klijentsku *Java Virtual Machine (JVM).*