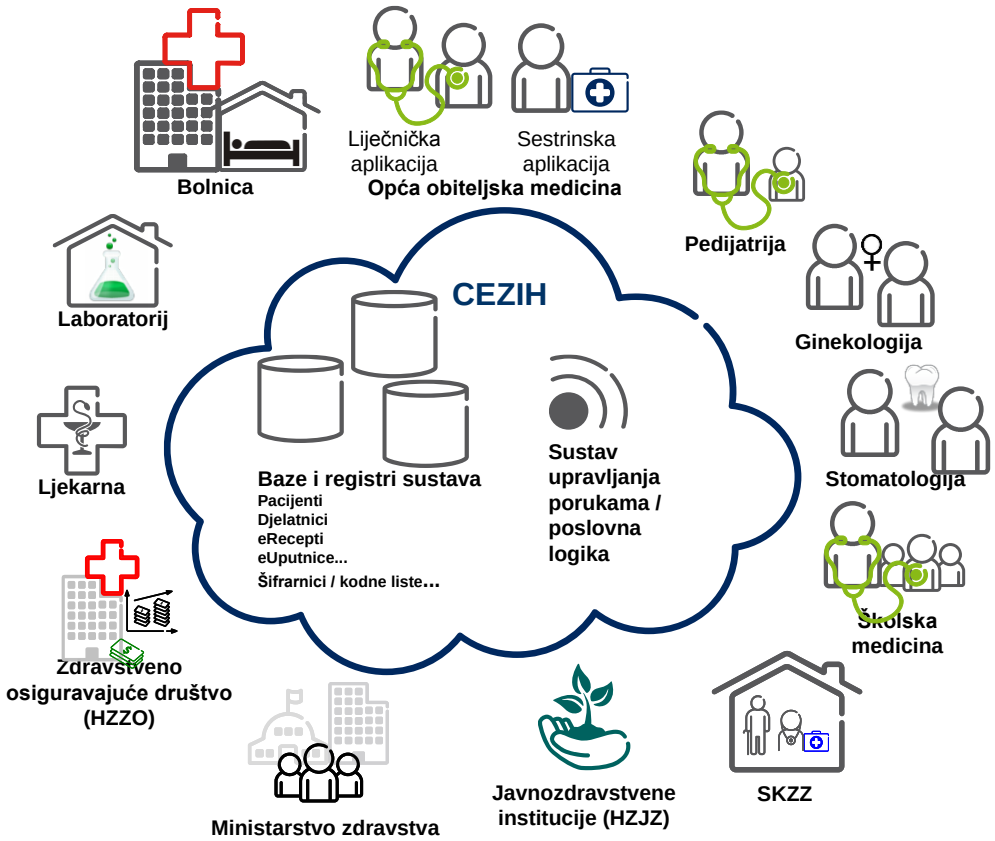
Autentifikacija korisnika te provjera administrativnih podataka - Funkcijska specifikacija

Centralni zdravstveni informacijski sustav Republike Hrvatske (CEZIH)

FUNCTION SPEC.



Sadržaj

1 Uvod

1.1 Svrha dokumenta

Svrha ovog dokumenta je specificiranje funkcionalnosti sustava CEZIH vezane za proces provjere prava pristupa korisnika servisima sustava te dohvat administrativnih podataka pacijenata.

1.2 Reference

[1] „Centralni zdravstveni informacijski sustav Republike Hrvatske (CEZIH) - Koncept sustava“; dok. br. 2/15517-FCPBA 101 24/8 Uhr

[2] 1/10260-FAP 901 0481 Uen Rev PC2 - *G1 User Implementation Guideline*– detaljni opis funkcionalnosti

2 Opis funkcionalnosti

2.1 Uvod

Prije korištenja bilo kojeg servisa CEZIH G1 sustava svaki klijent (G1_User) treba uspješno proći proces autentifikacije. Autentifikacija se zasniva na digitalnim certifikatima koji su izdani od strane HZZO-a svim pružateljima zdravstvenih usluga (liječnici opće prakse, medicinske sestre, Gx aplikacije, itd.). Bez odrađenog procesa autentifikacije neće biti dozvoljen pristup niti jednom drugom servisu koje CEZIH G1 sustav pruža.

Nakon uspješno odrađenog procesa autentifikacije pružatelji zdravstvenih usluga mogu pristupiti servisima CEZIH G1 sustava. Kod pružanja zdravstvenih usluga pacijentima, izvršava se provjera osobnih podataka i statusa osiguranja pacijenta. CEZIH G1 sustav daje mogućnost provjere tih podataka pomoću servisa dohvata administrativnih podataka.

2.2 Opis funkcionalnosti središnjeg sustava CEZIH

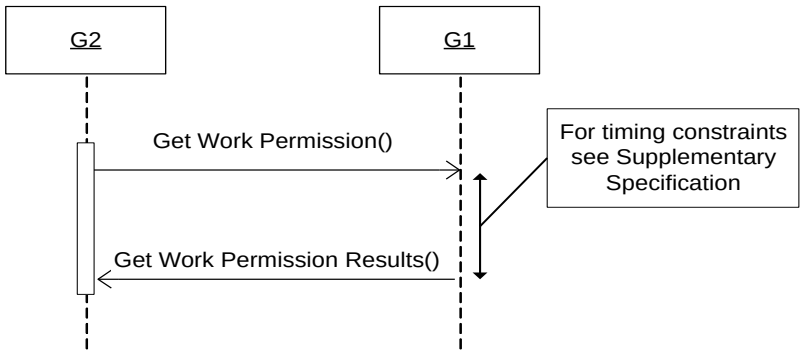
2.2.1 Autentifikacija korisnika

2.2.1.1 Storyboard

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

Svi detalji implementacije korisničkog slučaja su detaljno navedeni u dokumentu [2] 1/10260-FAP 901 0481 Uen Rev PC2 - *G1 User Implementation Guideline*– detaljni opis funkcionalnosti koji je u izvorniku pisan na engleskom jeziku ali će u ovom dokumentu biti prevedeni bitni detalji.

2.2.1.2 Dijagram slijeda



Slika 1 "Get Work Permission" dijagram slijeda

Slika 1 prikazuje dijagram slijeda za slučaj uporabe „Get Work Permission“. Ona se sastoji od dva značajna dijela:

- **Korisnička autorizacija**; identifikacija korisnika prema CEZIH G1 sustavu. Podrazumijeva slanje korisničkog certifikata sa smart kartice prema CEZIH G1 sustavu te provjera identiteta

- **Sistemsku autorizacija**; prema prepoznatom identitetu zdravstvenog djelatnika (iz poslanog korisničkog certifikata), G1 sustav Gx aplikaciji dodjeljuje odgovarajuću sistemsku ulogu u komunikaciji (Nurse_G2, MD_G2).

Rezultat poziva „Get Work Permission“ servisa se klijentu vraća sinkrono kao što je prikazano na dijagramu Slika 1.

U slučaju uspješne autentifikacije korisniku se dodjeljuje token u obliku web cookie-a koji se treba koristiti kod narednih poziva servisa CEZIH G1 sustava. U slučaju neuspješne autentifikacije sustav pozivatelju servisa vraća poruku o neuspjeloj autentifikaciji. U tom slučaju će i svi slijedeći pozivi drugim servisima CEZIH G1 sustava biti neuspješni zbog nepostojanja ispravnog autentifikacijskog tokena.

Detalji procedure dodjele autentifikacijskog tokena se nalaze u poglavlju 2.2.1.5 SSO mehanizam

2.2.1.3 Definicija XML poruka koje realiziraju interakcije u korisničkom slučaju

Tablica 1 definira detalje strukture poruka koje sudjeluju u interakcijama koje realiziraju korisnički slučaj.

	Initial Interaction (Get Work Permission)	**Response Interaction** (Get Work Permission rezultat)
Interaction Id	PRPM_IN000100	PRPM_IN100100
XML Schema for composite message	PRPM_IN000100.xsd	PRPM_IN100100.xsd
Transport Wrapper Message Type	MCCI_MT000100	MCCI_MT000300
Control Act Wrapper Message Type	MCAI_MT700201	MCAI_MT700203
Message Payload Message Type	PRPM_MT000100	PRPM_MT100100

Tablica 1 Definicija elemenata inicijalne i povratne poruke za poziv servisa "Get Work Permission"

2.2.1.4 Definicija web servisa

Slijedeća tablica prikazuje web servise koji sudionici u korisničkom slučaju pozivaju te koji sustavi sudjeluju u komunikaciji.

Web Servis	G1	G2_Application	HI_IS	PHC_IS
PRPM_AR100100_Service	Server (PRPM_AR100100.wsdl)	Client (PRPM_AR100100.wsdl)	Client (PRPM_AR100100.wsdl)	Client (PRPM_AR100100.wsdl)

Tablica 2 Definicija servisa korisničkog slučaja

2.2.1.5 SSO mehanizam

CEZIG G1 sustav je razvijen i konfiguriran da pruža podršku za „Single Sign On“ autentifikaciju korisnika (nadalje u tekstu SSO). SSO je mehanizam koji omogućuje da korisnik jednom odradi proces provjere prava pristupa CEZIH G1 sustavu te koristi servise sustava bez obzira na platformu na kojoj su servisi i aplikacije implementirani što povećava efikasnost cijelog sustava i jednostavnost korištenja servisa.

U CEZIH G1 sustavu SSO je implementiran na razini web servisa. Inicijalna autentifikacija i autorizacija pružatelja zdravstvenih usluga (korisnik, G2_User) se obavlja kod poziva servisa „Get Work Permission“. Korisnik se autentificira putem ispravnog X.509 digitalnog certifikata. Nakon uspješnog poziva „Get Work Permission“ servisa autentifikacija je uspješno izvršena te je dodijeljen token za G2_User-a. Ovaj token bi se trebao koristiti kod svih slijedećih poziva CEZIH G1 servisa. Bez korištenja dodijeljenog token-a kod poziva servisa korisnik neće imati prava pristupa servisima.

Inicijalna autentifikacija se izvodi u nekoliko koraka. Korisnik vrši prvi poziv „Get Work Permission“ servisa. Veza se ostvaruje preko HTTPS komunikacijskog kanala prema servisima koji su implementirani na web sloju aplikativnih poslužitelja. Vrši se uspostava SSL kanala. SSL sesija bi se trebala održati sa strane klijenta a tako i sa strane poslužitelja. U ovom trenutnu G2_User još uvijek ne posjeduje autentifikacijski token pa se vrši preusmjeravanje poziva na Access Manager poslužitelj. Access Manager poslužitelj odrađuje autentifikaciju (provjeru korisničkih podataka). Proces uspostave SSL kanala se ponavlja sa dodatnom provjerom klijentskog X.509 digitalnog certifikata. Nakon uspješne provjere korisničkog certifikata generira se SSO token. Token se korisniku dostavlja putem web cookie-a. Generirani cookie korisnik bi trebao zadržati do njegovog isteka ili do kraja korištenja Gx aplikacije. Slijedeći korak je preusmjeravanje poziva korisnika natrag prema web sloju aplikativnih poslužitelja. U ovom trenutnu korisnički poziv servisa sadrži i dodijeljeni cookie pa se poziv servisa „Get Work Permission“ uspješno odrađuje. Kod slijedećih poziva servisa korisnik bi trebao u pozivu koristiti dodijeljeni cookie te SSL sesiju uspostavljenu kod prvog poziva. Na osnovu generiranog token-a CEZIH G1 sustav može biti siguran da je korisnik koji poziva servis autentificiran te da sustav može dopustiti pristup štićenim resursima na osnovu dodijeljenih prava pristupa.

Korištenjem ovog mehanizma smanjena je količina podataka koja se šalje preko kanala. Jedino za vrijeme poziva servisa „Get Work Permission“ se vrši zahtjevna operacija uspostave SSL kanala i autentifikacije klijenta. Slijedeći pozivi servisa se vrše preko već uspostavljene SSL sesije koristeći izdani token. Vrlo je važno da G2_User implementira poziv servisa na opisani način. Ako se web cookie-i koji sadrže token-e za autentifikaciju i identifikaciju sesije ne koriste, moguće je uspješno pozvati samo „Get Work Permission“ servis. Pozivi prema ostalim servisima neće biti uspješno obavljeni. Nakon vremenskog isteka izdanog token-a pozivi servisa će biti onemogućeni te je potrebno ponovo izvršiti autentikaciju korisnika pozivom „„Get Work Permission“ servisa.

Skupina token-a koji omogućavaju održavanje sesije te SSO mehanizma su JSESSIONID, amFilterParam te iPlanetDirectoryPro.

2.2.1.6 XML digitalni potpis (XML Digital Signature)

Svaka poruka koja pošalje između CEZIH G1 sustava i vanjskih sustava koji koriste njegove servise treba biti digitalno potpisana korištenjem XML Digital Signature specifikacije definirane od strane W3C organizacije. Digitalni potpis se koristi u slijedeće svrhe:

- osiguranje integriteta poruke ili dijela poruke te
- u svrhu neporecivosti poslanih podataka

U porukama se potpisuje jedino dio poruke koji sadrži medicinske podatke.

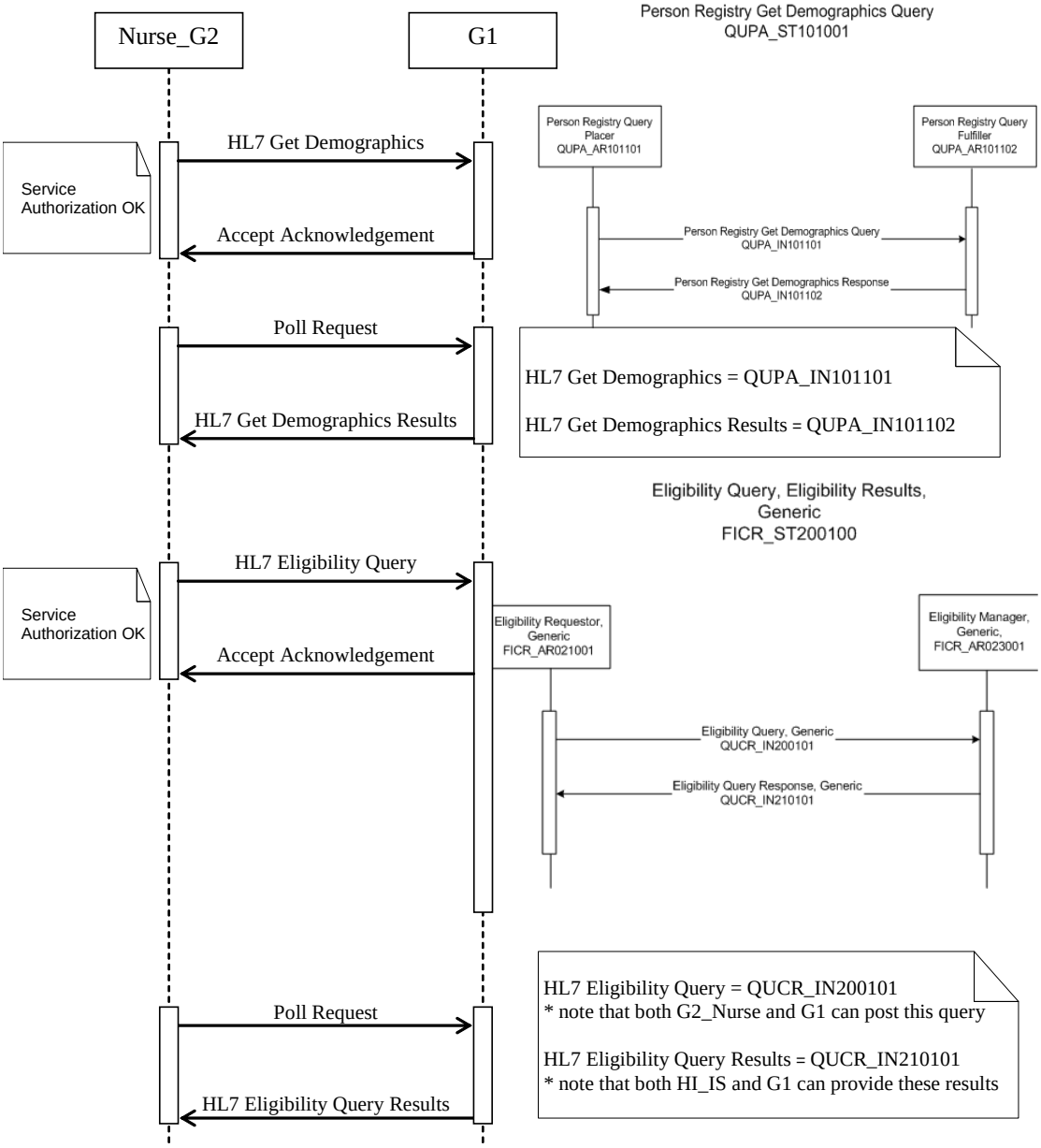
2.2.2 Dohvat administrativnih podataka

2.2.2.1 Storyboard

Kod obrade pacijenta od strane zdravstvenog djelatnika jedan od prvih akcija koja se obavi je pojašnjena u korisničkom slučaju “Dohvat podataka o pacijentu” (eng. “Retrieve Patient Info”). Korisnički slučaj se sastoji od dva dijela:

- **Dohvat pacijentovih administrativnih podataka (eng. „Get Demographics“)**; servis is vrši dohvat osnovnih pacijentovih administrativnih podataka u svrhu provjere identiteta
- **Provjera statusa osiguranja (eng. “ Eligibility Query“)**; servis vrši provjeru statusa osiguranja pacijenta

Slika 2 prikazuje dijagram slijeda poziva koji realizira korisnički slučaj „Dohvat administrativnih podataka“. Oba poziva servisa su asinkrona što znači da se prvo poziva pojedinačni servis a iza toga se vrši poziv servisa „poll“ mehanizma koji provjerava ima li za pozivatelja kakva nedohvaćena „poll“ poruka.



Slika 2 Dohvat podataka pacijenta

2.2.2.2 Interakcija „Dohvat administrativnih podataka pacijenta“

2.2.2.2.1 Dijagram slijeda

Dijagram slijeda interakcije je definiran na slici Slika 2

2.2.2.2.2 Definicija XML poruka koje realiziraju interakcije u korisničkom slučaju

Tablica 3 definira detalje strukture poruka koje sudjeluju u interakcijama koje realiziraju korisnički slučaj

	Initial Interaction (Person Registry Get Demographics Query)	**Response Interaction** (Person Registry Get Demographics Response)
Interaction Id	QUPA_IN101101	QUPA_IN101102
XML Schema for composite message	QUPA_IN101101.xsd	QUPA_IN101102.xsd
Transport Wrapper Message Type	MCCI_MT000100	MCCI_MT100300
Control Act Wrapper Message Type	QUQI_MT020001	QUQI_MT130000
Message Payload Message Type	QUPA_MT101101/ QUPA_MT101103	QUPA_MT101102

Tablica 3 Definicija elemenata poruke za poziv servisa "Get Demographics"

2.2.2.2.3 Definicija web servisa

Slijedeća tablica prikazuje web servise koji sudionici u korisničkom slučaju pozivaju te koji sustavi sudjeluju u komunikaciji.

Web Service	**G1**	**G2_Application**	**HI_IS**	**PHC_IS**
QUPA_AR101102_Service	Server (QUPA_AR101102.wsdl)	Client (QUPA_AR101102.wsdl)	N/A	N/A

Tablica 4 Definicija servisa korisničkog slučaja

2.2.2.3 Interakcija „Provjera osiguranja pacijenta“

2.2.2.3.1 Dijagram slijeda

Dijagram slijeda interakcije je definiran na slici Slika 2

2.2.2.3.2 Definicija XML poruka koje realiziraju interakcije u korisničkom slučaju

Slijedeća tablica definira detalje strukture poruka koje sudjeluju u interakcijama koje realiziraju korisnički slučaj

	Initial Interaction (Eligibility Query, Generic)	**Response Interaction** (Eligibility Query Response, Generic)
Interaction Id	QUCR_IN200101	QUCR_IN210101
XML Schema for composite message	QUCR_IN200101.xsd	QUCR_IN210101.xsd
Transport Wrapper Message Type	MCCI_MT000100	MCCI_MT100300
Control Act Wrapper Message Type	QUQI_MT020001	QUQI_MT120001
Message Payload Message Type	QUCR_MT200101	QUCR_MT210101

2.2.2.3.3 Definicija web servisa

Slijedeća tablica prikazuje web servise koji sudionici u korisničkom slučaju pozivaju te koji sustavi sudjeluju u komunikaciji.

Web Service	**G1**	**G2_Application**	**HI_IS**	**PHC_IS**
FICR_AR021001_Service	Server (FICR_AR021001.wsdl)	N/A	Client (FICR_AR021001.wsdl)/ Server (FICR_AR021001_EX.wsdl)	N/A
FICR_AR023001_Service	Server/ client (FICR_AR023001.wsdl)	Client (FICR_AR023001.wsdl)	Client (FICR_AR023001.wsdl)/ Server (FICR_AR023001_EX.wsdl)	N/A

Tablica Definicija servisa korisničkog slučaja