Pregled sustava za umrežavanje i računalno upravljanje EKG dijagnostičkim postupkom

Sedlar, Zoran

Undergraduate thesis / Završni rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University North / Sveučilište Sjever**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:122:473696

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-25**

Repository / Repozitorij:

University North Digital Repository

Sveučilište Sjever

Završni rad br. 365/EL/2015

Pregled sustava za umrežavanje i računalno upravljanje EKG dijagnostičkim postupkom

Zoran Sedlar, 1547/601

Varaždin, rujan 2015. godine

Sveučilište Sjever

Odjel Elektrotehnike

Završni rad br. 365/EL/2015

Pregled sustava za umrežavanje i računalno upravljanje EKG dijagnostičkim postupkom

Student

Zoran Sedlar, 1547/601

Mentor

mr. sc. Matija Mikac

Varaždin, rujan 2015. godine

Sveučilište Sjever
Sveučilišni centar Varaždin
104. brigade 3, HR–42000 Varaždin

UNIVERSITY NORTH

Prijava završnog rada

Definiranje teme završnog rada i povjerenstva

ODJEL: Odjel za elektrotehniku

PRISTUPNIK: Zoran Sedlar | MATIČNI BROJ: 1547/601

DATUM: 22.09.2015

KOLEGIJ: Računalne mreže

NASLOV RADA: Pregled sustava za umrežavanje i računalno upravljanje EKG dijagnostičkim postupkom

MENTOR: Matija Mikac | ZVANJE: viši predavač

ČLANOVI POVJERENSTVA:
1. Ladislav Havaš
2. Stanko Vincek
3. Matija Mikac

Zadatak završnog rada

VŽ KC

MMI

BROJ: 365/EL/2015

OPIS

Standardni dijagnostički postupci poput elektrokardiograma (EKG) odavno su poznati i korišteni. Korištenje računalnih i mrežnih tehnologija omogućilo je razvoj složenijih sustava za umrežavanje i upravljanje većim brojem uređaja, s ciljem povećanja fleksibilnosti u samom provođenju postupka dijagnostike.

U završnom radu je potrebno proučiti i dokumentirati konkretni sustav primjenjiv u bolničkim centrima, te pokušati provesti osnovnu analizu "crne kutije" (obzirom na zatvorenost sustava od strane proizvođača) - detektirati osnovne korake postupka i provjeriti pretpostavke vezane uz mrežnu komunikaciju i dostupnost baze podataka...

U završnom radu je potrebno:

* opisati sustav za upravljanje EKG uređajima, SEMA
* opisati dijelove sustava, kao i koncept korištenja
* uočiti osnovne elemente sustava vezane uz mrežnu komunikaciju i povezati ih sa standardnim mrežnim tehnologijama
* dati pregled osnovnih postavki sustava, kao i detalje o implementaciji sustava u medicinskoj ustanovi
* prikazati dio funkcionalnosti administracijskog sučelja sustava, ukazati na osnovne mogućnosti testiranja statusa
* ovisno o mogućnostima, provesti analizu mrežnog prometa za određene korake standardiziranog postupka
* ovisno o mogućnostima, razmotriti strukturu baze podataka, navesti ograničenja ovisno o ovlastima korisnika
* prema tehničkoj dokumentaciji sustava proučiti strukture standardno korištenih datoteka, kao i dostupne detalje sustava - dokumentirati i, po mogućnosti, na primjerima razmotriti strukturu datotečnih zapisa

ZADATAK URUČEN: 29.09.2015 | POTPIS MENTORA: M. Mikac

REPUBLIKA HRVATSKA 4 KOPRIVNICA SVEUČILIŠTE SJEVER

SVEUČILIŠTE SJEVER

Predgovor

Zahvaljujem mentoru mr. sc. Matiji Mikacu na vodstvu, korisnim savjetima i usmjeravanju pri izradi završnog rada.

Zoran Sedlar

Sažetak

U radu je opisan sustav SEMA, švicarskog proizvođača Schiller, namijenjen umrežavanju i računalnom upravljanju EKG dijagnostičkim sustavom. U prvom dijelu rada dan je osvrt na glavne značajke ovog sustava, te razlike između pojedinih licenci unutar sustava. Opisano je međusobno povezivanje između SEMA sustava i bolničkog informacijskog sustava, te je prikazan protok podataka između ta dva sustava.

U drugom dijelu rada dan je pregled osnovnih elemenata sustava i njihovih funkcionalnosti, s naglaskom na mogućnosti administriranja korištenjem sučelja dostupnog osoblju zaduženom za instalaciju i nadzor rada.

U trećem dijelu rada dan je prikaz osnovne strukture podataka dostupnih krajnjim korisnicima. Obavljeno snimanje mrežne komunikacije koje je omogućilo ograničenu analizu samog komunikacijskog protokola unutar segmenta SEMA sustava vezanog za pristup podacima o korisnicima. Obzirom da se radi o zaštićenoj komunikaciji, detaljna analiza nije bila moguća, što je, nažalost, potvrđeno i kroz e-mail komunikaciju s proizvođačem sustava, kojom je utvrđeno da se svi bitni parametri koji bi se mogli iskoristiti za detaljniji tehnički opis sustava predstavljaju poslovnu tajnu.

Popis korištenih kratica

EKG Elektrokardiogram

HL-7 Health Level 7

DICOM Digital Imaging and Communications in Medicine

PACS Picture Archiving and Communication System

HIS Hospital Information System

IP Internet Protocol

SSH Secure Shell

GDT Global Descriptor Table

Sadržaj

1. UVOD ... 1

1.1 SPECIJALIZIRANI PROTOKOLI ... 3

2. SEMA SUSTAV ... 4

2.1. SEMA SOLO ... 4
2.2. SEMA DIAGNOSTIC ... 4
2.3. 2.3 SEMA WORKSTATION ... 4

3. PREGLED ELEMENATA SUSTAVA ... 8

3.1. MREŽNA KOMUNIKACIJA ... 9

4. PREGLED PROTOKA PODATAKA ... 10

5. SEMA POSLUŽITELJ ... 14

6. KOMUNIKACIJSKI POSLUŽITELJ ... 17

7. LICENCNI POSLUŽITELJ ... 21

8. APLIKACIJSKI POSLUŽITELJ ... 23

9. POSLUŽITELJ ZA POVEZIVANJE ... 26

9.1. OSNOVNI TIJEK RADA ... 26
9.2. MIRTH FILTERI ... 29
9.3. MIRTH TRANSFORMERI ... 29
9.4. MIRTH KONEKTORI ... 30
9.5. RANIJE VERZIJE POSLUŽITELJA ZA POVEZIVANJE ... 30

10. ORGANIZACIJA PODATAKA ... 32

11. KOMUNIKACIJA PUTEM INTERNETA ... 37

11.1. TRANSPORTNI SLOJ ... 38
11.2. AUTENTIFIKACIJSKI SLOJ ... 38
11.3. SPOJNI SLOJ ... 39
11.4. DOPUNA SSH SIGURNOSTI ... 39
11.5. SNIMANJE PROMETA ... 39

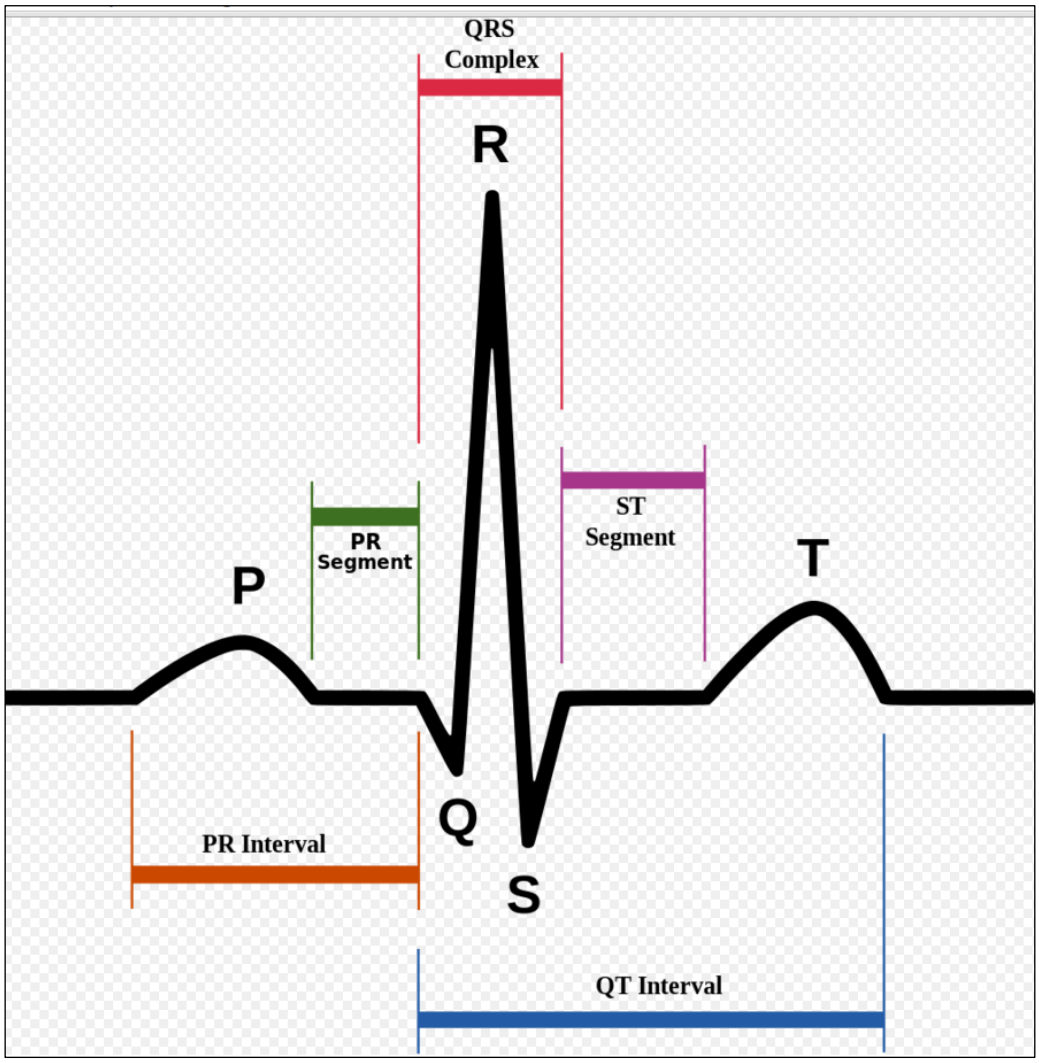
12. ZAKLJUČAK ... 42

13. LITERATURA ... 43

1. Uvod

Elektrokardiogram ili skraćeno EKG je signal kojeg dobivamo kada EKG mjerni instrument (elektrokardiograf) bilježi električnu aktivnost srca u vremenu. Srcem prolazi impuls koji se širi u tkiva oko srca, te se ta razlika potencijala može izmjeriti na koži. EKG mjerni instrument pomoću elektroda postavljenih na kožu čovjeka može zabilježiti razliku potencijala. Mjerenje se obavlja korištenjem 12 izvoda koje dijelimo u dvije skupine: periferne i (I, II, III, aVR, aVL, aVF) i prekordijalne izvode (V1, V2, V3, V4, V5, V6). Normalni EKG se sastoji od P-vala, QRS-kompleksa i T-vala.

Prikaz pojedinačnog otkucaja srca zabilježenog EKG-om, sa naznačenim karakterističnim parametrima dan je na slici 1.1. [1]



Slika 1.1 Prikaz EKG signala

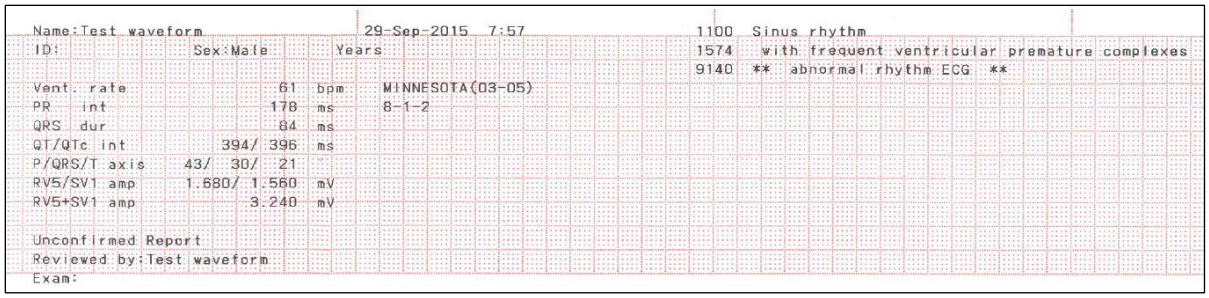
Trajanje EKG signala ili RR interval (vremenski razmak između dva R) iznosi između 0,6 i 1,2 sekunde kod zdravih osoba koje imaju između 50 i 100 otkucaja srca u minuti.

EKG mjerni instrument je izumio nizozemski liječnik Willem Einthoven 1903. godine, te je za to otkriće dobio Nobelovu nagradu za medicinu 1924 godine. Pošto

elektrokardiogram ima vrlo važno mjesto u medicini, proizvodnja EKG mjernih uređaja se povećala, a i sami uređaji su napredovali od svojih početaka, te u današnje vrijeme EKG mjerni instrumenti imaju više funkcija i mogućnosti, npr. odabir dobne skupine pacijenta, spol pacijenta, ispis interpretacije dobivenoga signala itd.

Slika 1.2 Prikaz EKG signala dobivenog prilikom mjerenja EKG mjernim instrumentom (skenirano)

Na slici 1.2 je prikazan izmjeren EKG signal kojeg smo dobili pomoću simulatora. Simulator EKG signala se koristi kod servisa EKG mjernih uređaja kad je potrebno utvrditi ispravnost tzv. „pacijent kabla“ (kabla sa elektrodama). Na slici 1.3 su prikazane vrijednosti izmjerenog signala, te je dan prikaz interpretacije (dijagnoza) dobivenog signala.



Slika 1.3 Prikaz interpretacije EKG signala koju daje EKG mjerni instrument (skenirano)

Sljedeći logičan korak u razvoju EKG uređaja je bio da se proizvođači okrenu mogućnostima koje nudi suvremena IT tehnologija. Iz toga je proizašla ideja za povezivanjem EKG mjernih instrumenata na zajednički poslužitelj (engl. *server*) i izradu sustava koji mogu detaljnije analizirati sam elektrokardiogram (EKG). U ovom završnom radu je opisano jedno od takvih IT rješenja, a to je sustav SEMA, švicarskog proizvođača *Schiller* .

Preduvjet postavljanja sustava SEMA jest instalacija i konfiguracija standardnih podsustava: poslužitelja baze podataka (MySQL), Java programskog okruženja (JDK/JRE) i aplikacijskog poslužitelja (Glassfish). Sam sustav, osim standardnih mrežnih protokola, za razmjenu informacija i komunikaciju sa drugim sustavima podržava HL-7 i DIACOM protokole.

1.1 Specijalizirani protokoli

HL-7 (engl. *Health Level 7*) predstavlja skup protokola koje koriste softverske aplikacije različitih bolnica i zdrastvenih ustanova za prijenos podataka o pacijentima i za prijenos raznih drugih administrativnih podataka. Pošto bolnice i zdrastvene ustanove koriste različite računalne sustave za svoje potrebe potrebno je da svi ti sustavi međusobno komuniciraju radi što bržeg pronalaženja željene informacije. [2]

DIACOM (engl. *Digital Imaging and Communications in Medicine*) je standard koji služi za upravljanje, arhiviranje i slanje podataka koji sadrže medicinske vizualizacije (npr. RTG slike, EKG slike, CT slike itd.). DIACOM koristi IP protokol za komunikaciju između različitih sustava, te omogućuje integriranje skenera, poslužitelja (engl. *server*), radne stanice i pisača različitih proizvođača u zajednički sistem za komunikaciju i arhiviranje slika (engl. *Picture Archiving and Communication System*). [3]

2. SEMA sustav

Funkcija SEMA sustava je upravljanje, analiza i pohrana podataka EKG-a u mirovanju (engl. *resisting ECG*), ritam EKG-a (engl. *rhytam ECG*), te EKG-a pod opterećenjem (engl. *stress ECG*). Sustav SEMA podržava isključivo Microsoft Windows platformu i dostupan je u više verzija. SEMA je dizajnirana da se može koristiti za samostalne mjerne instrumente i za računalno bazirane mjerne instrumente. Postoje tri verzije SEMA sustava:

1. SEMA Solo
2. SEMA Diagnostic
3. SEMA Workstation

2.1. SEMA Solo

„SEMA Solo“ koristi se za samostalna snimanja i pohranu EKG snimaka. Ova verzija nema mogućnost mrežnog rada, pa se sve snimke pohranjuju lokalno.

2.2. SEMA Diagnostic

„SEMA Diagnostic“ je potpuno umrežen EKG upravljački sustav za pregled, snimanje i analizu EKG snimaka snimljenih mjernim uređajima. Pristup poslužitelju je moguć sa bilo kojeg računala koje je uključeno u SEMA sustav - ova verzija sustava omogućuje rad samo jednog korisnika.

2.3. SEMA Workstation

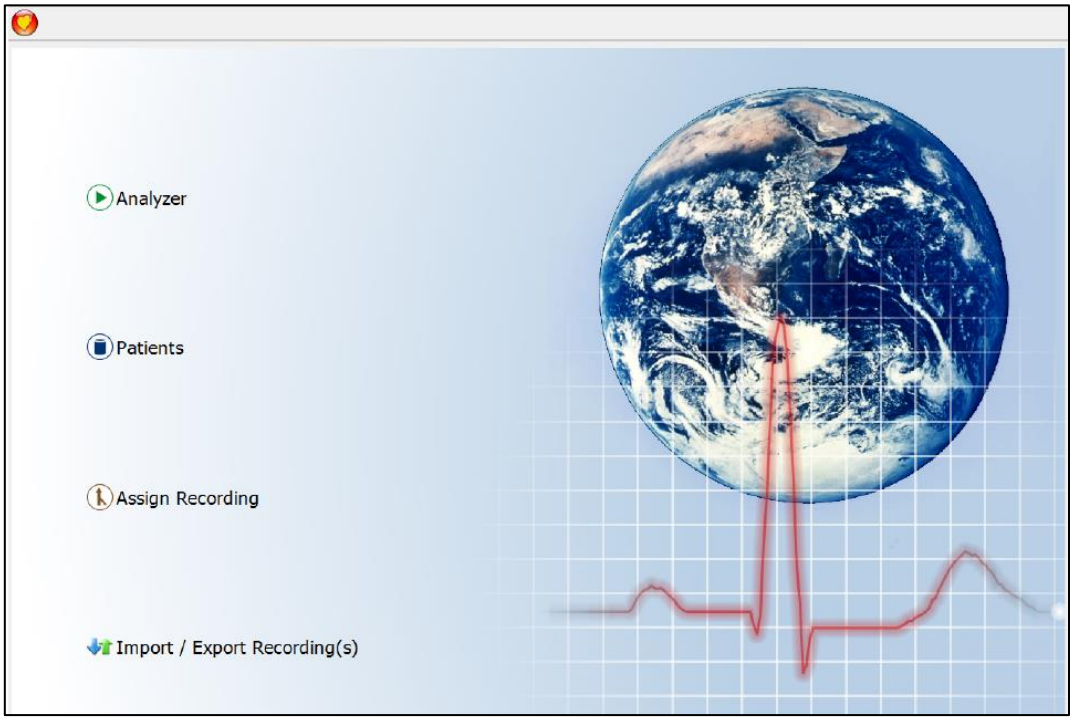
„SEMA Workstation“ je potpuno umrežen EKG upravljački sustav sa proširenim funkcijama upravljanja. „SEMA Workstation“ sustav ima plutajući sustav dozvola (engl. *floating licence system*) koji ima mogućnost pristupa poslužitelju sa bilo kojeg računala na mreži, uz valjanu dozvolu za pristup. Broj plutajućih dozvola (engl. *floating licence*) je 5 do 250 i određuje broj korisnika kojima je omogućena istovremena prijava na poslužitelj.

Kada je prijavljen maksimalni broj korisnika, dodatna prijava nije moguća tako dugo dok se neki korisnik ne odjavi s poslužitelja (engl. *user log off*).

Moguće su tri vrste licenci (dozvola) za korištenje „SEMA Workstation“ verzije sustava:

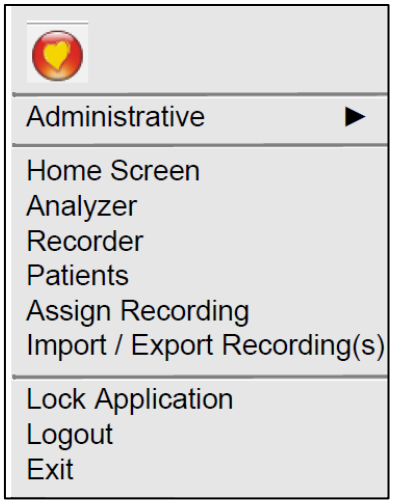
1. SEMA Office – broj korisnika od 2 do 4 (prijavljenih istovremeno)
2. SEMA Professional – broj korisnika od 5 do 20 (prijavljenih istovremeno)
3. SEMA Enterprise – broj korisnika od 25 do 250 (prijavljenih istovremeno)

Pristup u program se ostvaruje nakon prijave važećom lozinkom, nakon čega nam se otvara početna stranica programa (slika 2.1).



Slika 2.1 Početna stranica programa

Prilikom pritiska na logo u lijevom gornjem dijelu prozora, otvara se prozor koji daje na odabir neke mogućnosti za rad (slika 2.2).

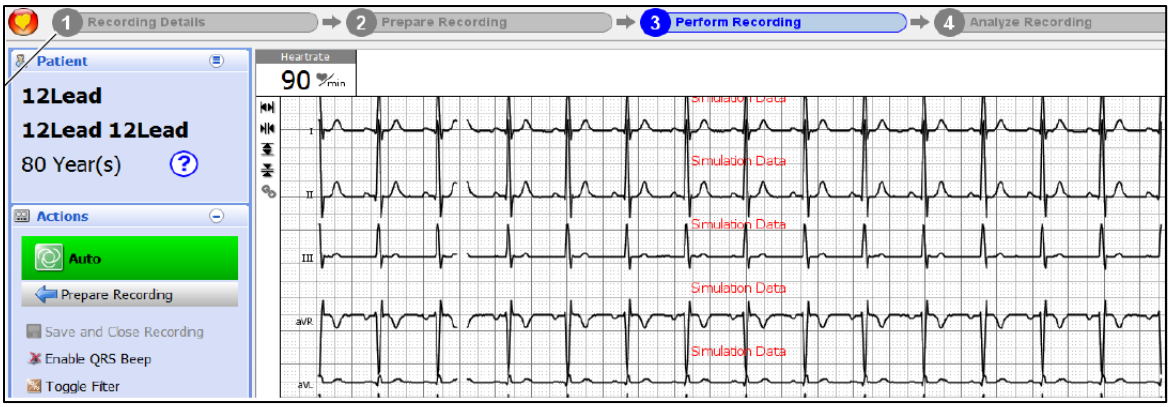


Slika 2.2 Prikaz izbornika za odabir postavki sistema

Dostupne stavke izbornika i njihove funkcionalnosti:

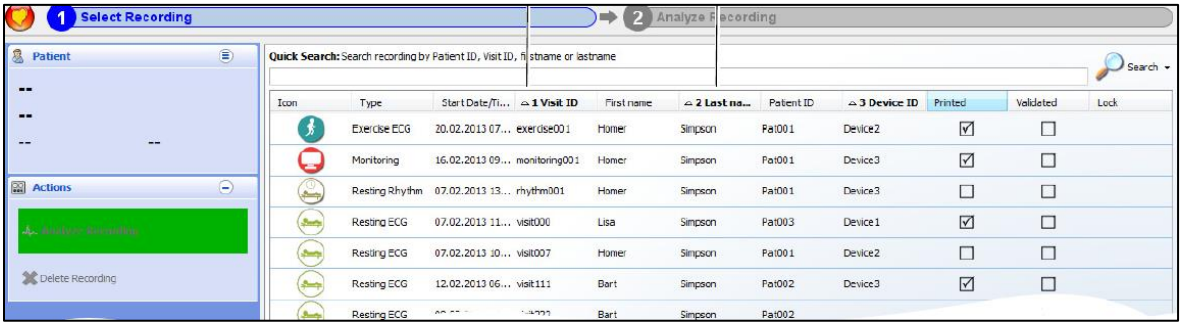
1. *Administrative* – postavke sustava (vidljivo samo kod prijave tehničke podrške, standardni korisnik nema pristup)
2. *Home Screen* – povratak na početnu stranu (slika 2.1)

3. *Analyzer* – pretraživanje, pregled i interpretacija snimaka
4. *Recorder* – pretraživanje popisa pacijenata u bazi podataka
5. *Patients* – kreiranje novog pacijenta, izmjena postojećih podataka o pacijentu
6. *Assign Recording* – odabir pretrage
7. *Import/Export Recordings* – unos snimaka u sustav i prijenos izvan sustava
8. *Lock Application* – zaključavanje aplikacije
9. *Logout* – odjava iz sustava



Slika 2.3 Prikaz prozora EKG pretrage

Slika 2.3 prikazuje izgled prozora prilikom izvođenja EKG pretrage. Nakon što je pretraga završena, kompletna EKG snimka pretrage se može detaljno pregledati, može se zumirati točno određeni dio signala (u kojem je uočena anomalija ili se jednostavno želi detaljnije pregledati dio signala), te se taj isti dio može kasnije ispisati. Takav pristup omogućuje lakše uočavanje anomalija i lakše i preciznije utvrđivanje dijagnoze pacijenta.



Slika 2.4 Prikaz korisničkog sučelja

Slika 2.4 prikazuje korisničko sučelje koje prikazuje osnovne podatke o pacijentima i provedenim postupcima. Standardno se prikazuju ime i prezime pacijenta, njegov identifikacijski broj (engl. *patient ID*), broj uređaja (ukoliko ih ima više) na kojem je napravljen pregled (engl. *device ID*), te simbolički prikaz izvršenih pretraga.

Na slici 2.5 su prikazani svi simboli koji se koriste u SEMA sustavu za označavanje standardnih/podržanih pretraga.

Slika 2.5 Prikaz simbola za pojedine pretrage

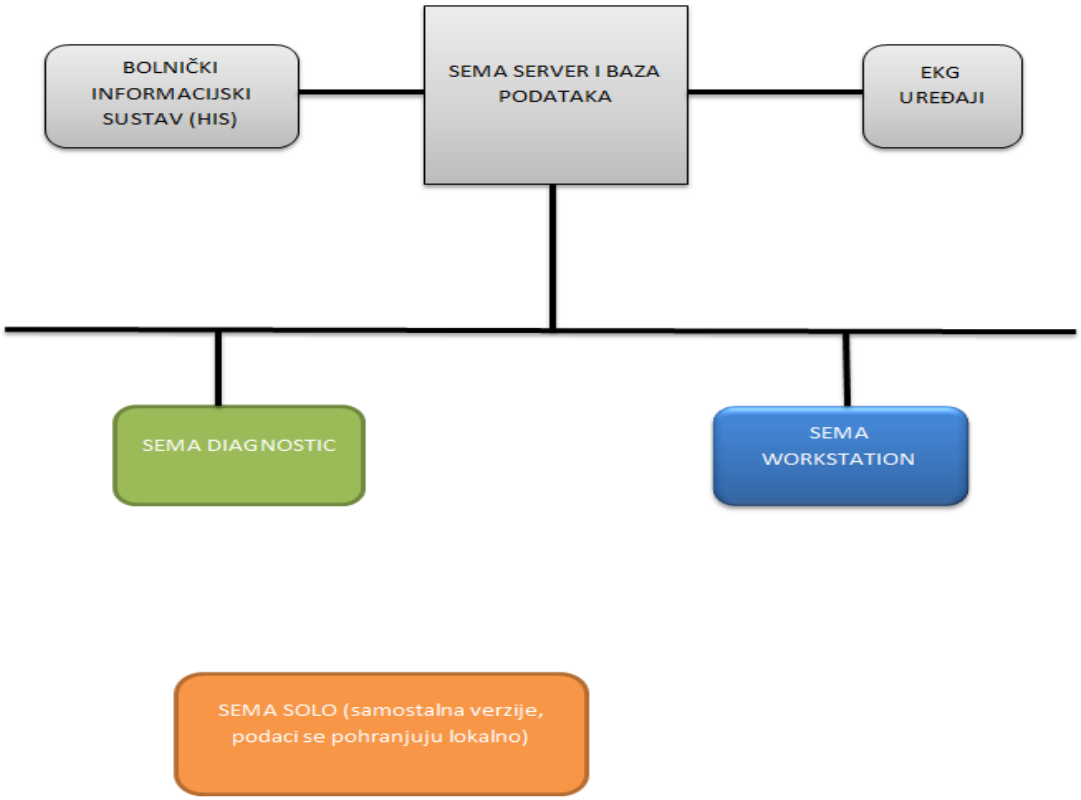
SEMA sustav podržava praćenje i evidentiranje sljedećih pretraga:

- EKG u mirujućem stanju (engl. *Resting EKG*)
- Mjerenje pulsa u mirujućem stanju (engl. *Resting Rythm*)
- EKG pod opterećenjem (engl. *Exercise EKG*)
- Mjerenja u hitnim slučajevima
- Spirometrija
- Ergo spirometrija (spirometrija pod opterećenjem)
- Holter EKG (može biti 24 sata ili 48 sati)
- Holter tlaka (može biti 24 sata ili 48 sati)

Pošto svaka od navedenih pretraga ima oznaku (simbol) koji stoji uz ime pacijenta, liječniku je vrlo jednostavno i pregledno iz popisa odabrati željenu pretragu i inerpretirati ju. Takvim načinom rada postiže se ušteda na vremenu i točnost podataka (ne može doći do zabune da se pomiješaju ili izgube nalazi pretrage).

3. Elementi sustava

Na slici 3.1 prikazan je odnos dostupnih verzija licenci SEMA sustava. Vidljiva je stalna povezanost podsustava za pohranu podataka sa (SEMA poslužitelj) „SEMA Diagnostic“ i „SEMA Workstation“, kao i povezanost bolničkog informacijskog sustava sa podsustavom za pohranu podataka. Također je vidljivo da verzija „SEMA Solo“ nema nikakvih veza sa SEMA podatkovnim podsustavom, a samim time ni sa bolničkim informacijskim sustavom - sve snimke napravljene tom verzijom sustava arhiviraju se lokalno, tj. na uređaju kojim su rađene snimke.



Slika 3.1 Prikaz povezivanja licenci SEME

Za komunikaciju između SEMA poslužitelja i EKG uređaja, te vanjskih poslužitelja koriste se:

- SEMA poslužitelj (engl. *SEMA Server*)
- Komunikacijski poslužitelj (engl. *Communication Server Light*)
- Plutajući poslužitelj za licence (engl. *Flooting Licence Server (FLS)*)
- Aplikacijski poslužitelj (engl. *Glassfish*)
- Poslužitelj za povezivanje (engl. *Connectivity Server (Mirth)*)

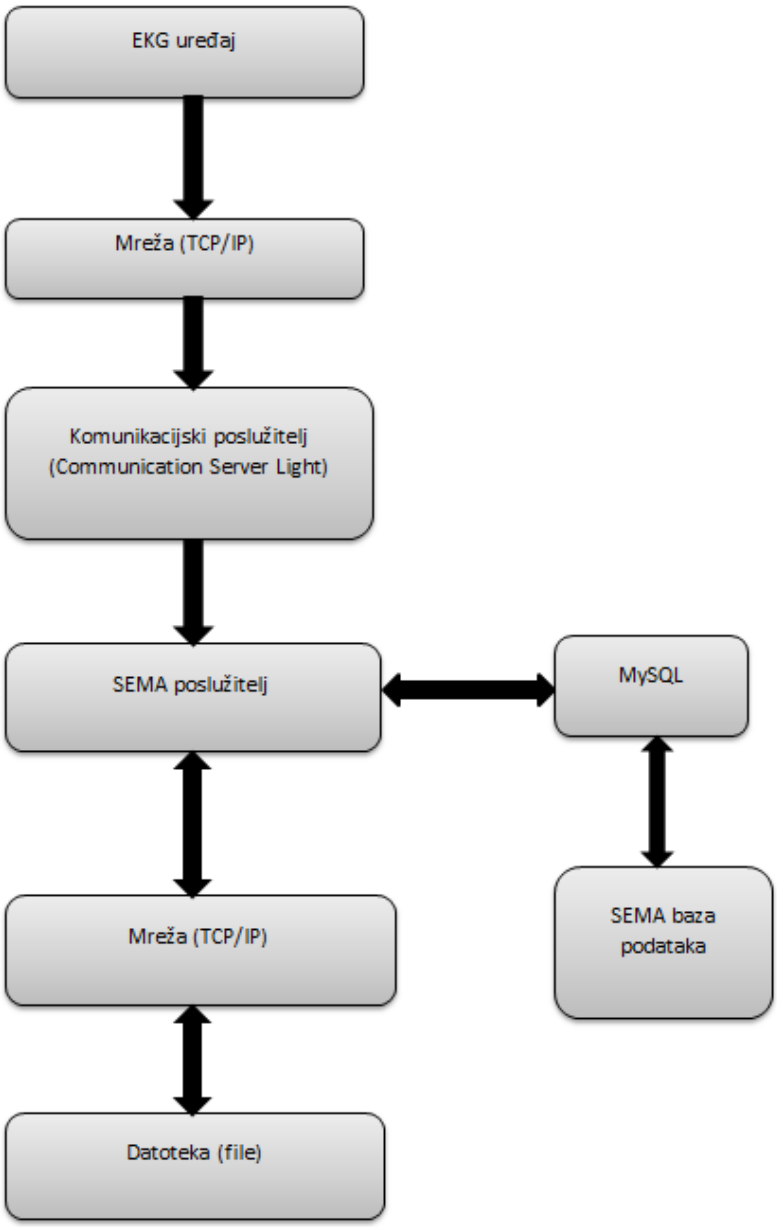
3.1. Mrežna komunikacija

Za komunikaciju između EKG uređaja i komunikacijskog poslužitelja koriste se standardni protokoli – na mrežnom sloju koristi se IP (v4) protokol, na transportnom sloju TCP (engl. *Transmission Control Protocol*), a za realizaciju sigurne komunikacije koriste se uobičajena rješenja bazirana na TLS protokolu (engl. *Transport Layer Security*). Podaci koji se prenose (aplikacijski sloj) i koriste u SEMA sustavu su specifičnih formata koje proizvođač smatra poslovnom tajnom. [1]

4. Pregled protoka podataka

U nastavku je dan pregled protoka podataka između EKG uređaja i SEMA poslužitelja. Pregled sadržava tri moguće situacije:

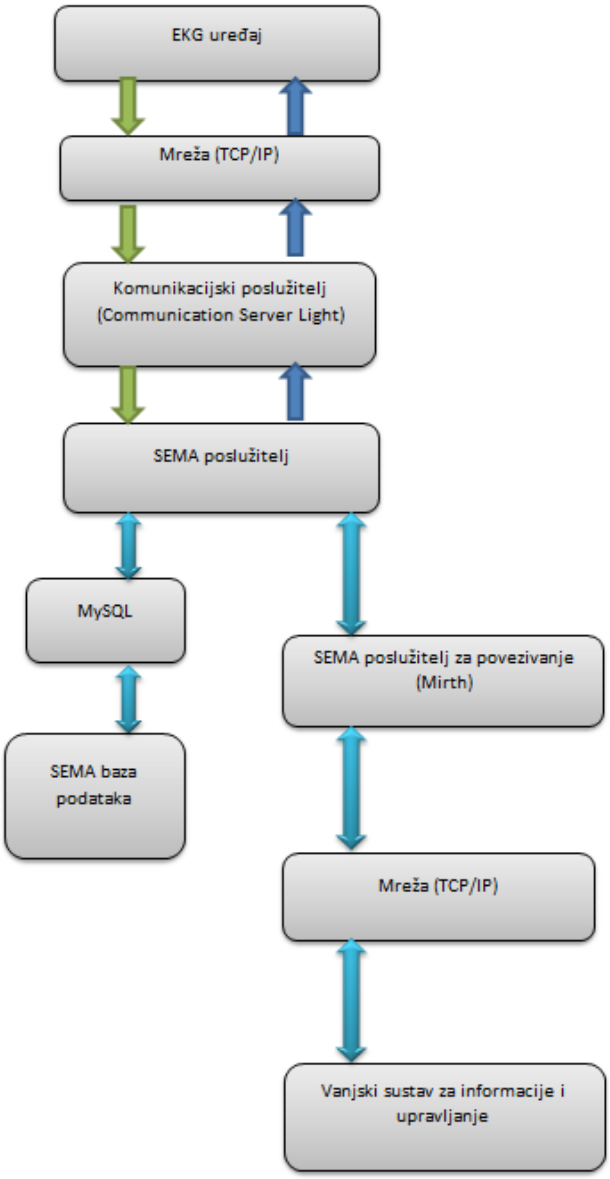
- slanje rezultata snimanja s uređaja na računalo uključeno u SEMA sustav
- slanje zahtjeva za dohvat informacija o pacijentu (engl. *Pacient Data Query*)
- slanje zahtjeva za dohvat radne liste (engl. *Worklist*)



Slika 4.1 Prikaz protoka podataka od EKG uređaja do računala

Na slici 4.1 prikazan je pregled protoka EKG snimke od EKG uređaja pa do računala u SEMA sustavu na kojemu je pomoću SEMA aplikacija snimka vizualizirana. EKG uređaj šalje rezultate snimanja na mrežu (Internet) preko koje se podaci šalju na

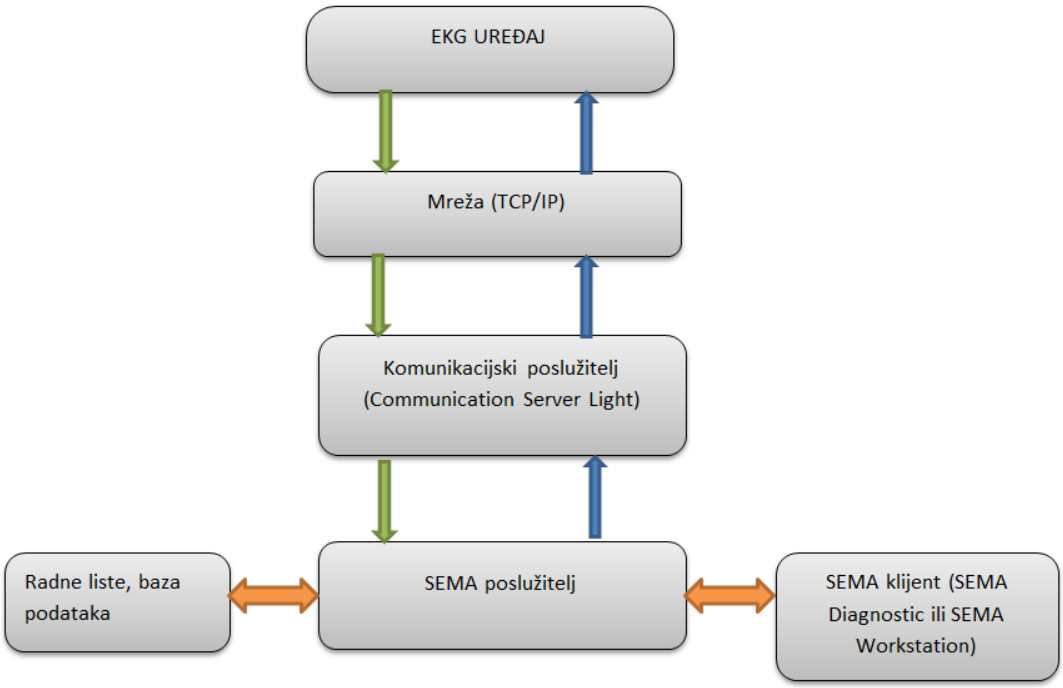
komunikacijski poslužitelj. Komunikacijski poslužitelj prima podatke, te ih obrađuje i pretvara u SEMA format kojim se koristi SEMA poslužitelj. SEMA poslužitelj podatke (EKG snimku) šalje u bazu podataka, gdje se ona pohranjuje kod točno određenog pacijenta definiranog identifikacijskim brojem. EKG snimka dostupna za pregledavanje i uređivanje u sustavu SEMA i to u „SEMA Diagnostic“ ili „SEMA Workstation“.



Slika 4.2 Prikaz protoka zahtjeva za podacima o pacijentu

Na slici 4.2 prikazani je protok podataka kada se sa EKG uređaja pošalje zahtjev za podacima o pacijentu. Svakom pacijentu je dodijeljen broj pod kojim se spremaju njegovi podaci (ime, prezime, adresa, rezultati pretraga, dijagnoze, itd.). Kada komunikacijski poslužitelj primi zahtjev, on ga proslijedi SEMA poslužitelju. SEMA poslužitelj primi zahtjev i pokrene potragu za *Pacient ID* u bazi podataka. Pretraga može biti unutar SEMA baze podataka ili se pomoću SEMA poslužitelja za povezivanje (engl. *Mirth*) pretražuje vanjski sustav upravljanja i informacija. U tom

sustavu nalazi se baza podataka bolničkog informacijskog sustava (*engl. HIS*). Ako se pretraga izvršava unutar SEMA baze podataka tada se koristi identifikacijski broj pacijenta, a ako se koristi vanjski sustav tada SEMA poslužitelj za povezivanje definira format zahtjeva. Kada su pronađeni podaci o pacijentu bilo u SEMA bazi podataka bilo u vanjskom sustavu, oni pomoću SEMA poslužitelja i komunikacijskog poslužitelja dolaze do EKG uređaja.



Slika 4.3 Prikaz protoka zahtjeva za radnom listom

Slika 4.3 prikazuje protok podataka kada sa EKG uređaja pošaljemo zahtjev za „Radnom listom“. Pošto postoje EKG mjerni uređaji koji imaju više opcija snimanja EKG-a (u mirovanju, pod nekim naporom, npr. vožnja ergometarskog bicikla itd.), također imaju mogućnost snimanja saturacije kisika u krvi (SpO2), neinvazivno mjerenje tlaka itd., na radnoj listi je određena vrsta pretrage koja će se odraditi.

Informacije definirane u radnoj listi su:

1. Broj naloga (engl. *Order ID*) – jedinstvena identifikator naloga

2. Broj uređaja (engl. *Device ID*) – identifikator uređaja nad kojim se vrši nalog

3. Prioriteti – specificira prioritet : - *Undefined*
   - *Routine*
   - *High*
   - *Status (immediete)*

4. Željen postupak – definiramo postupak izvođenja mjerenja
    - *Undefined*
    - *Resting EKG*
    - *Exercise EKG*
    - *Monitoring*
    - *Spirometry*
    - *Holter EKG*
    - *Holter BP* (tlaka)

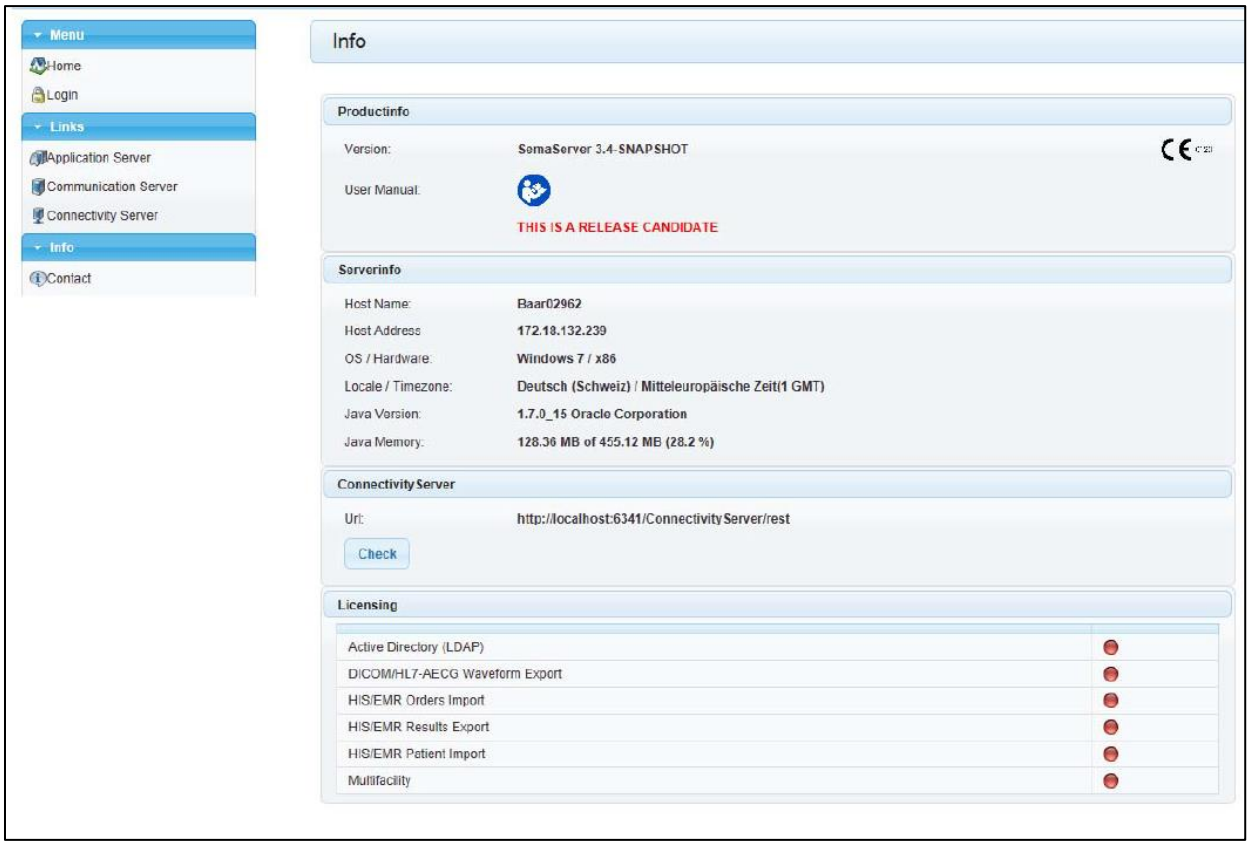
5. Status:
    a) *Off* - nalog poništen
    b) *To record* – nalog je spreman za slanje na EKG uređaj
    c) *Recording* – izvodi se snimanje na uređaj
    d) *To analyse* – snimka je poslana sa uređaja na poslužitelj i može se pregledati i analizirati
    e) *Analysing* – snimka je otvorena sa SEMA klijent programom
    f) *Finished* - snimka je pregledana i spremljena u bazu podataka
    g) *Cancelled* – unos otkazan
    h) *To assign* – unos je registriran za određenog pacijenta

Zahtjev se kroz mrežu uputi na komunikacijski poslužitelj koji zahtjev proslijedi SEMA poslužitelju. SEMA poslužitelj pretraži opću bazu podataka i bazu podataka za specifični uređaj sa kojeg je poslan zahtjev. Kada se pronađe točna radna lista SEMA poslužitelj putem komunikacijskog poslužitelja je šalje na uređaj sa kojeg je poslan zahtjev.

5. SEMA poslužitelj

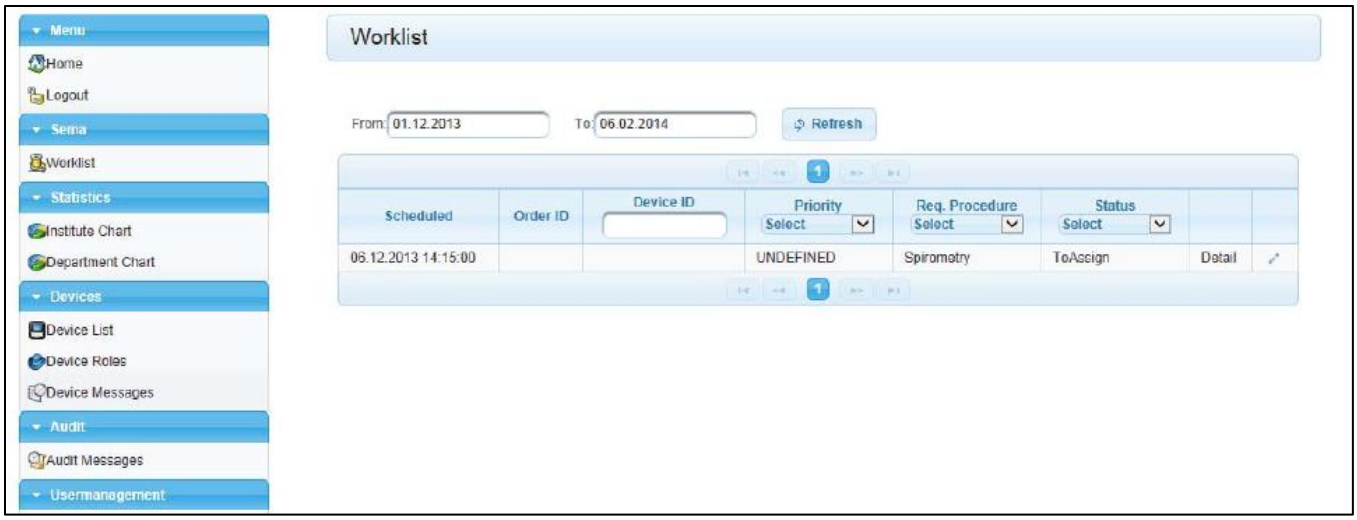
Tijekom normalnog rada, upravljanje podacima o pacijentu i EKG snimkama je unutar SEMA sustava, dok SEMA poslužitelj sinkronizira podatke i to radi u pozadini.

Početni prozor (slika 5.1) SEMA poslužitelja daje podatke o verziji, adresi, detalje o hardveru i statusu Java okruženja.



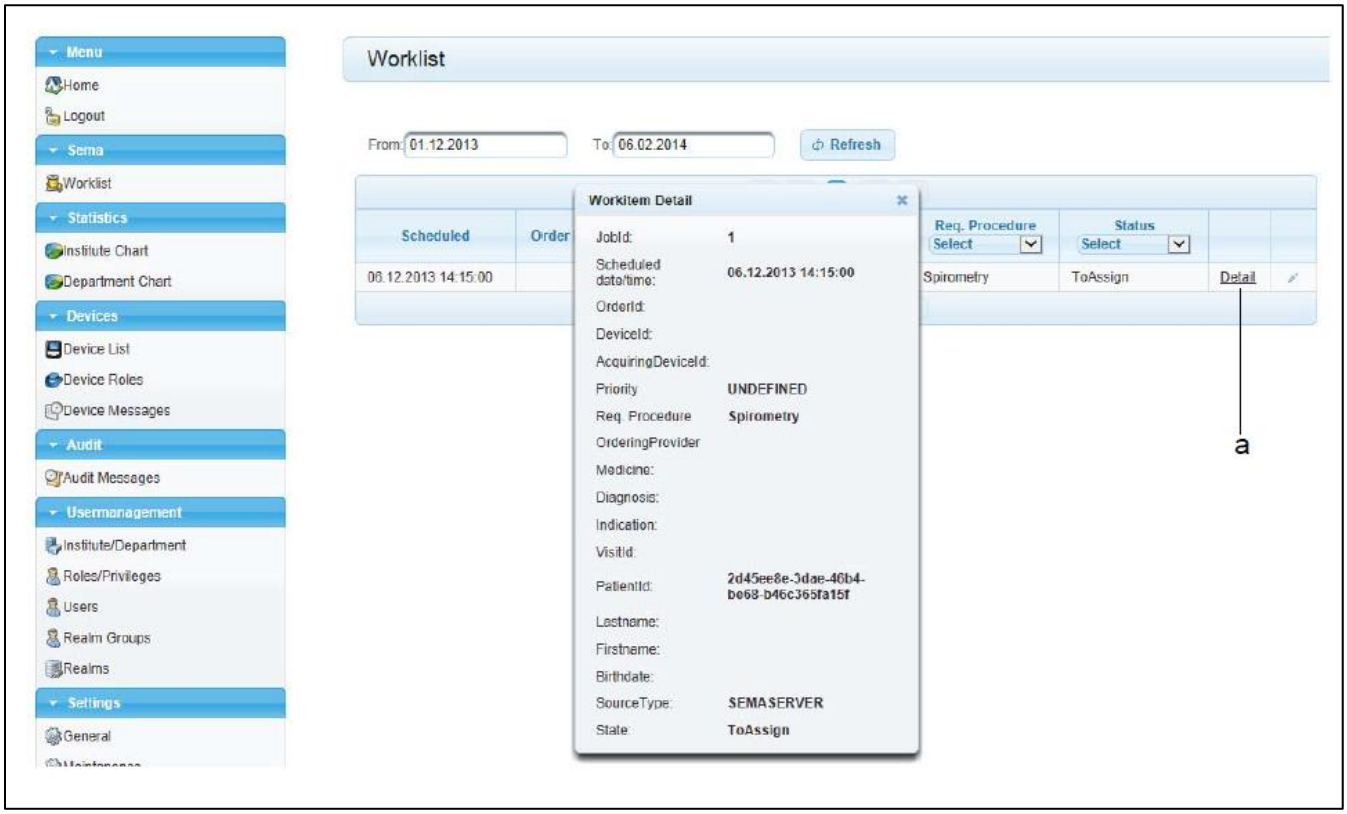
Slika 5.1 Prikaz početnog prozora

U izborničkoj grupi „*Links*“, dana je mogućnost izbora tipa poslužitelja na koji se korisnik (administrator) spaja, vrši nadzor i druge dozvoljene radnje, dok je u izborničkoj grupi „*Menu*“ dan izbor prijave. Nakon izvršene prijave administratoru su dane mogućnosti pregledavanja radnih lista i podataka o EKG uređajima unutar sustava SEMA.



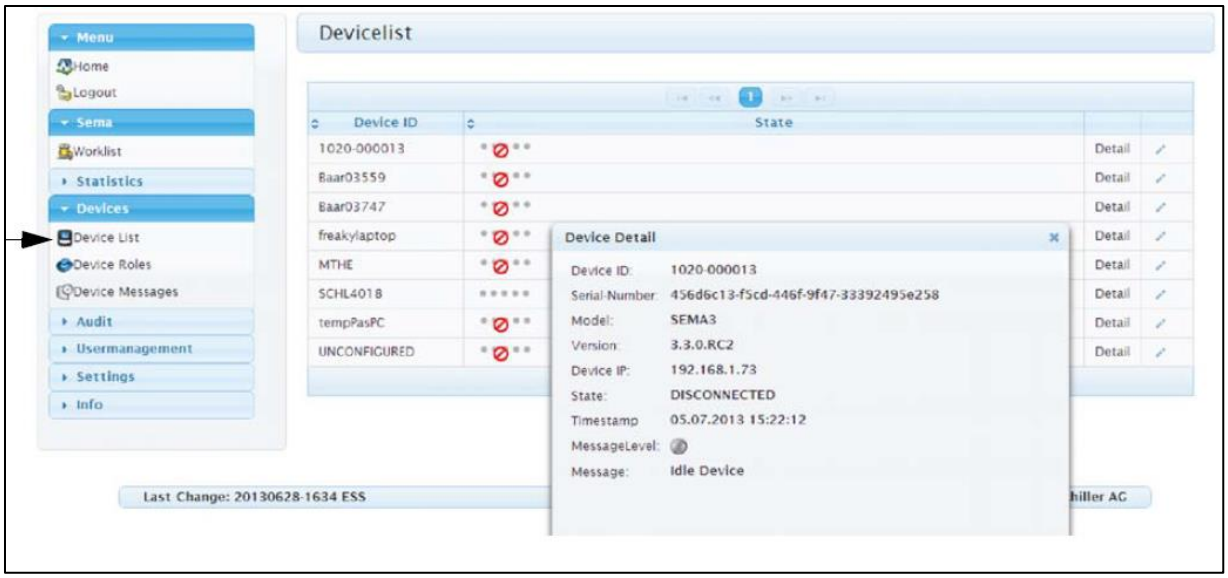
Slika 5.2 Prikaz popisa radne liste

Odabirom izborničke grupe „*Worklist*“ dobivamo popis radnih lista, na kojima je vidljiv trenutni status radne liste i tip pretrage koji će se izvoditi na EKG uređaju. (slika 5.2). Odabirom mogućnosti „*Detail*“ dan nam je detaljan uvid podataka vezan uz određenu radnu listu (slika 5.3).



Slika 5.3 Prikaz detalje radne liste

U izborničkoj grupi „*Device*“ dan nam je popis EKG uređaja unutra sustava SEMA (slika 5.4).

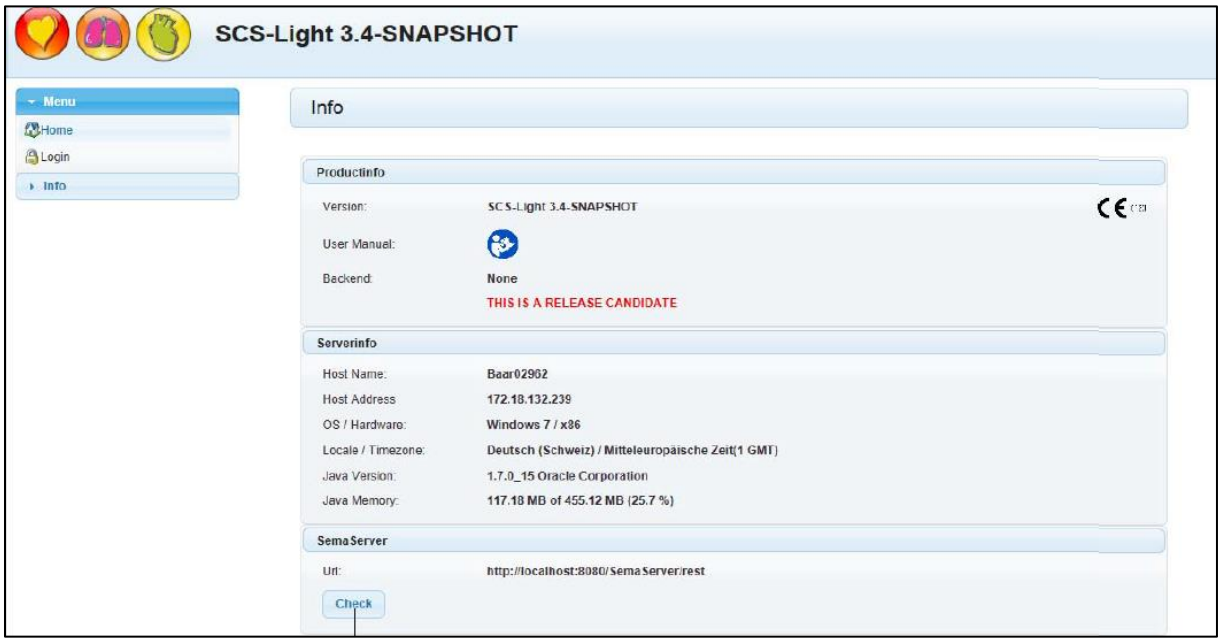


Slika 5.4 Prikaz popisa uređaja

Uz uređaje na popisu nalazi se izbornička grupa „*Detail*“ u kojoj su podaci poput idetifikacijskoga broja uređaja (engl. *Device ID*), njegovog statusa, IP adresa uređaja, verzija programa na uređaju, serijski broj uređaja itd. (slika 5.4). Pristup ovim podacima ograničen je samo na administratora, tj. tehničku službu za podršku koja ima posebno korisničko ime i lozinku koju koristi za prijavu u sustav SEMA. Iz prakse je poznato da je korisnicima (liječnici, medicinske sestre, medicinski tehničari itd.) važan rezultat pretrage, dok ove popratne informacije im nisu upotrebljive u njihovom radu. Pošto je cilj ovog sustava da olakša rad medicinskoga osoblja, baze podataka koje su njima dostupne su limitirane samo na podatke o pacijentu i sve snimke koje su ti pacijenti obavili pomoću sustava SEMA.

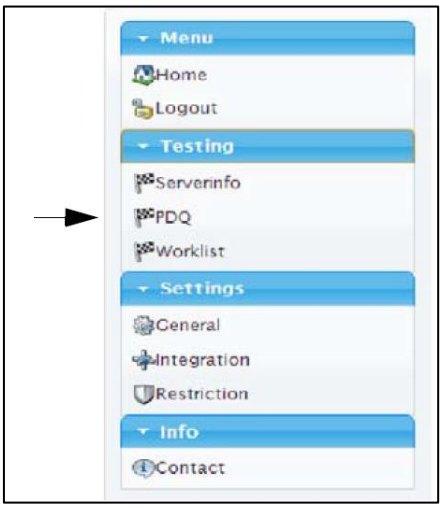
6. Komunikacijski poslužitelj

Komunikacijski poslužitelj je programsko sučelje za komunikaciju između mjernih EKG uređaja i SEMA poslužitelja. Prihvaća zahtjev za podacima o pacijentu i zahtjev za radnom listom, te služi za učitavanje i preuzimanje podataka u određenom formatu između SEMA poslužitelja i EKG uređaja. Komunikacijski poslužitelj djeluje samostalno u pozadini.



Slika 6.1 Prikaz početnog prozora

Provjera stanja povezanosti komunikacijskog poslužitelja izvršava se odabirom izbornika „*Check*“ . U izborničkom grupi „*Menu*“ dana je mogućnost prijave administratora, koji može vršiti nadzor rada komunikacijskog poslužitelja. U izborničkoj grupi „*Testing*“ odabire se funkcija za testiranje poslužitelja (slika 6.2).



Slika 6.2 Prikaz mogućnosti odabira

Testiranje poslužitelja se izvodi pomoću dvije funkcije::

- *PDQ* funkcija (podaci o pacijentu)
- *Worklist* funkcija (radna lista)

Program uspješno simulira vanjski uređaj i može potvrditi integritet veze (komunikacije) između komunikacijskog poslužitelja i SEMA poslužitelja. Testiranje se izvodi u dva koraka:

1. Pošaljemo zahtjeva za podacima o pacijentu sa identifikacijskim brojem pacijenta na komunikacijski poslužitelj i čekamo odgovor.
2. Pošaljemo zahtjev za radnom listom sa identifikacijskim brojem korisnika (komunikacijski poslužitelj i čekamo odgovor.

Ako je test uspješan pojavljuje se informacija prikazana na slici 6.3


```xml
  <?xml version="1.0" encoding="US-ASCII"?>
- <response>
  - <parameters>
    - <param>
        <name>PRODUCTINFO</name>
        <value>SCS-Light 3.2-SNAPSHOT</value>
      </param>
    - <param>
        <name>STATUS</name>
        <value>OK</value>
      </param>
    - <param>
        <name>REASON</name>
        <value>SUCCESSFUL</value>
      </param>
    - <param>
        <name>TODO</name>
        <value>TODO_SERVERINFO_REQUEST</value>
      </param>
    - <param>
        <name>TIMESTAMP</name>
        <value>2013-02-05T16:02:18.643+01:00</value>
      </param>
  </parameters>
</response>
```


Slika 6.3 Prikaz uspješno izvedenog testa

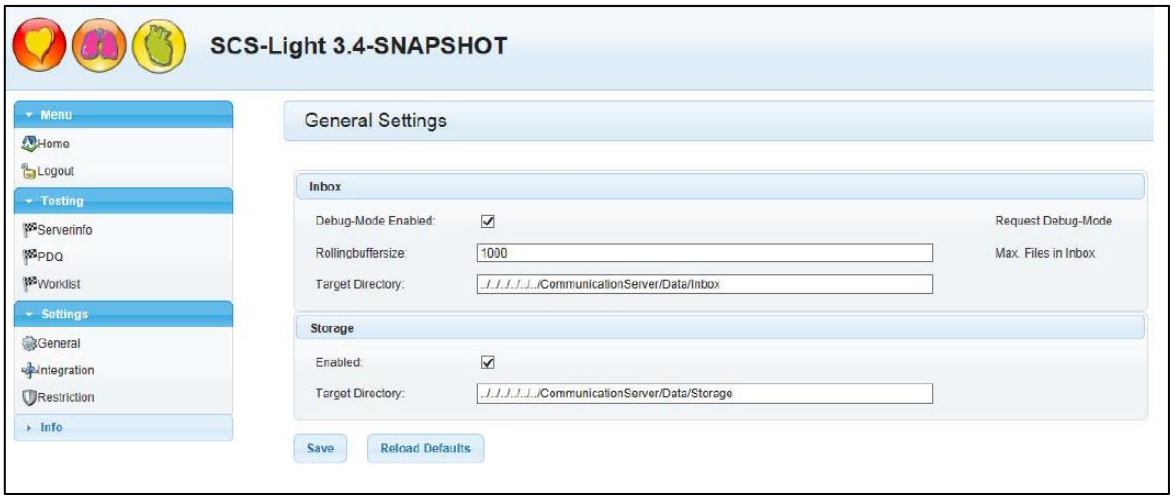
Ako je test neuspješan tada se pojavljuje sljedeća informacija (slika 6.4) , te je potrebno provjeriti sve postavke komunikacijskog poslužitelja i SEMA poslužitelja.

```xml
<?xml version="1.0" encoding="US-ASCII"?>
- <response>
  - <parameters>
    - <param>
        <name>STATUS</name>
        <value>REJECTED</value>
      </param>
    - <param>
        <name>REASON</name>
        <value>PDQ_NOT_RECOGNIZED</value>
      </param>
    - <param>
        <name>TODO</name>
        <value>TODO_DB_PATDATA_REQUEST</value>
      </param>
    - <param>
        <name>TIMESTAMP</name>
        <value>2013-02-05T16:15:00.143+01:00</value>
      </param>
  </parameters>
</response>
```


Slika 6.4 Prikaz neuspješno izvedenog testa

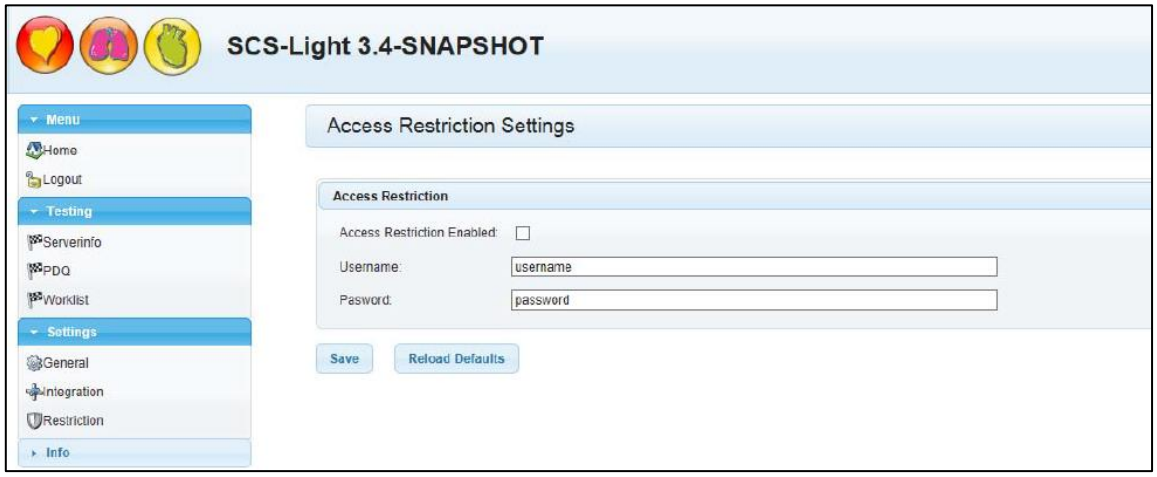
Generalne postavke komunikacijskog poslužitelja (slika 6.5) prikazuju ulazni spremnik i spremnik za pohranu.. Ulazni spremnik je mapa u kojoj su učitani svi zahtjevi poslani sa EKG uređaja na komunikacijski server. Postoje dva načina na koji se mogu pohraniti podaci:

1. Odabirom *Debug-Mode* svi zahtjevi će biti pohranjeni
2. Odabirmo Max.Files in Inbox definiramo maksimalni broja datoteka u ulaznom spremniku, radi kao *Rolling Buffer* (prva datoteka unutra, prva datoteka van).



Slika 6.5 Prikaz postavki komunikacijskog poslužitelj

Prilikom instalacije sustava SEMA potrebno je izvršiti navedene testove. Prijava administratora je prikazana na slici 6.6.



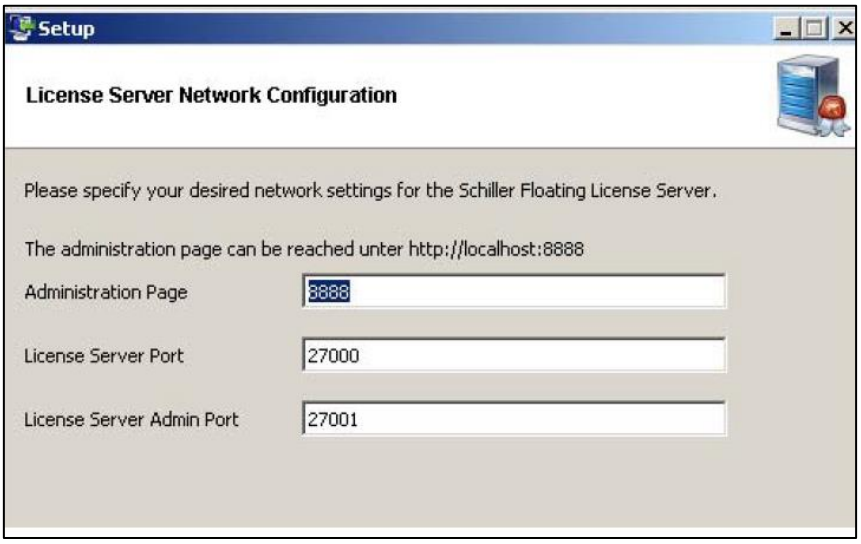
Slika 6.6 Prikaz prozora za prijavu

7. Licencni poslužitelj

Licencni poslužitelj u sustavu SEMA (verzija SEMA Workstation) je izveden kao tzv. plutajući poslužitelj (engl. *Flooting Licence Server)*. Kontrolira broj istovremeno prijavljenih korisnika (broj je ograničen) na SEMA poslužitelju. Nužno je da plutajući poslužitelj licenci bude instaliran na istom uređaju kao i SEMA poslužitelj. Moguće su tri verzije licenci (dozvola):

1. SEMA Office – broj korisnika od 2 do 4 (prijavljenih istovremeno)
2. SEMA Professional – broj korisnika od 5 do 20 (prijavljenih istovremeno)
3. SEMA Enterprise – broj korisnika od 25 do 250 (prijavljenih istovremeno)

Prilikom instalacije odabire se administratorska stranica i ulazi (port) koji će se koristiti (slika 7.1).

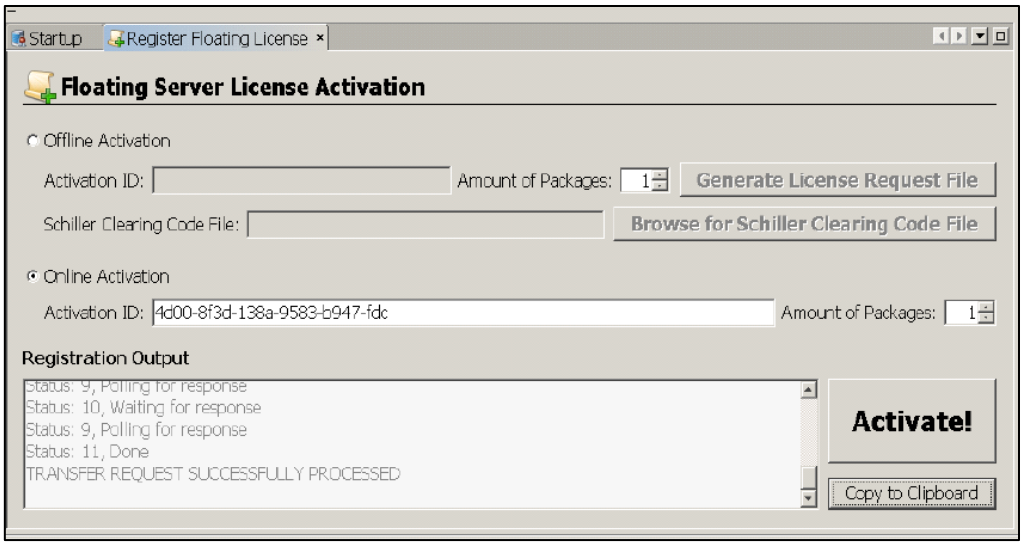


Slika 7.1 Prikaz prozora za konfiguraciju

Licenca se arhivira na SEMA poslužitelju, te je nemoguće istu licencu upotrebljavati tj. instalirati na više računala. Prije samog korištenja potrebno je aktivirati licencu. Aktivacija licence je moguća na 2 načina:

1. *Online*
2. *Offline*

Na slici 7.2 dan nam je prikaz aktivacije licence pomoću aktivacijskog broja (engl. *Activation ID)*.



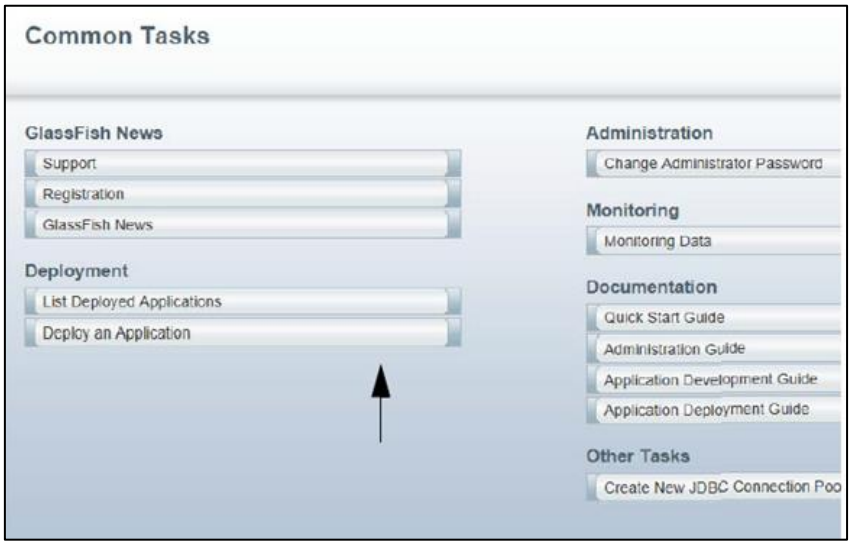
Slika 7.2 Prikaz prozora za aktivaciju

Nakon uspješne aktivacije, potrebno je da administrator izvrši provjeru funkcionalnosti licencnog poslužitelja. To se postiže tako da se ponovno pokrene računalo i izvrši uspješna prijava na SEMA poslužitelja, te se provjeri da li se aktivirana licenca nalazi na popisu (slika 7.3).

Slika 7.3 Prikaz popisa licenci

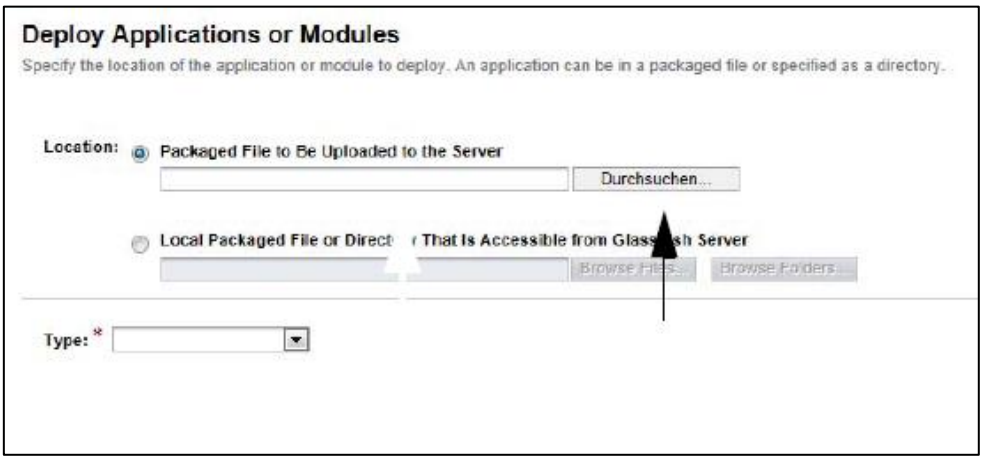
8. Aplikacijski poslužitelj

Glassfish je aplikacijski poslužitelj otvorenog tipa (engl. *open source*) koji koristi *Java EE 6* platformu, te podržava *Enterprise JavaBeans*, *JPA*, *JavaServer Faces* itd. Zahvaljujući tome može se vrlo lako i efikasno koristiti u poslovnim aplikacijama. Glavna zadaća aplikacijskog poslužitelja unutar sustava SEMA je kontrola komunikacije između EKG uređaja i SEMA poslužitelja. [7]
Prozor sa postavkama otvara se prilikom odabira „*Application Server*“ u izborničkoj grupi „*Links*“ (slika 8.1)



Slika 8.1 Prikaz početnog prozora

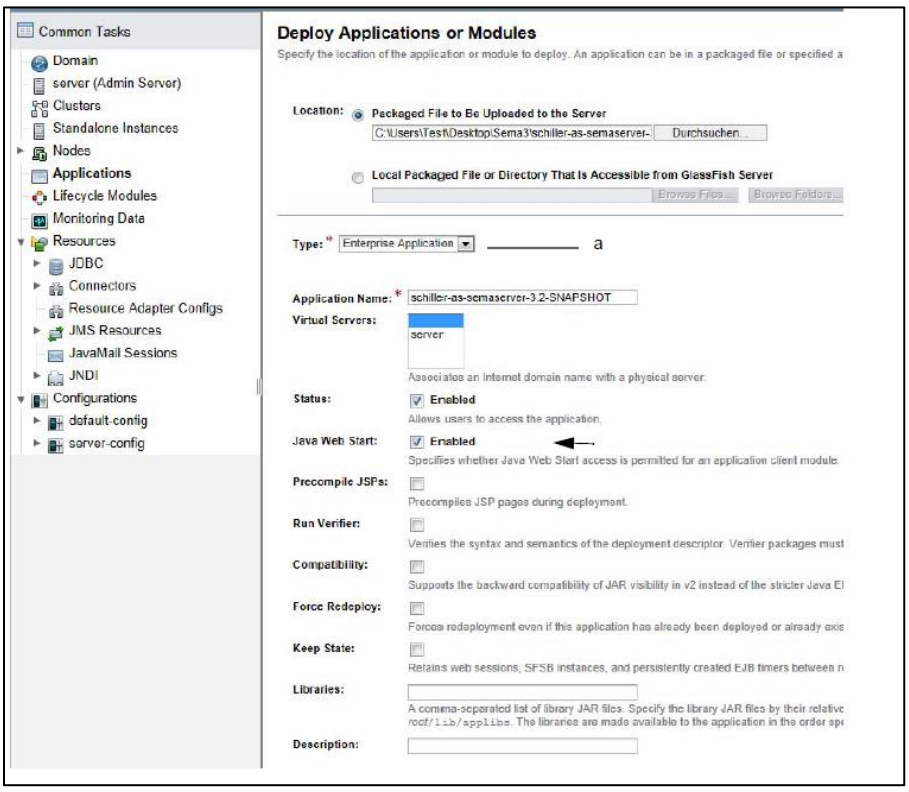
Odabirom „*Deploy an Application*“ u izborničkoj grupi „*Deployment*“ administrator određuje datoteku (lokaciju) na kojoj će se pohranjivati (spremati) podaci dobiveni na EKG uređaju koji se nalazi u sustavu SEMA (slika 8.2).



Slika 8.2 Prozor za raspoređivanje

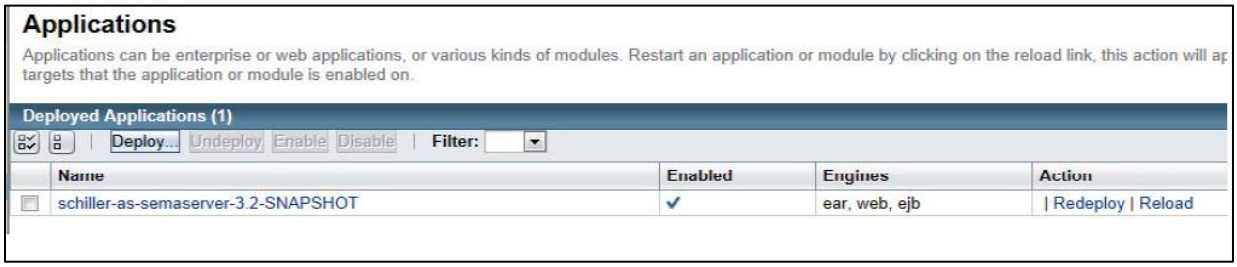
Osim lokacije pohrane podataka, izvršava se odabir imena aplikacije (engl. *Application Name*) , te postavke koje su potrebne za uspješnu komunikaciju između

EKG uređaja i SEMA poslužitelja. Postavke u izborničkoj grupi „*Type*“ su interne postavke poizvođača sustava SEMA i nesmiju se mjenjati (slika 8.3).



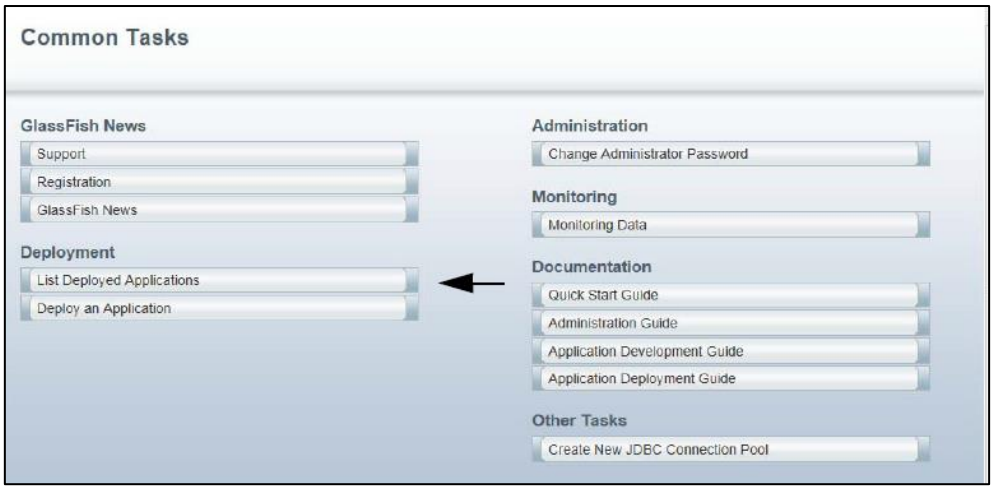
Slika 8.3 Prikaz prozora za odabir postavki

Slika 8.4 daje prikaz raspoređene aplikacije za SEMA poslužitelja.



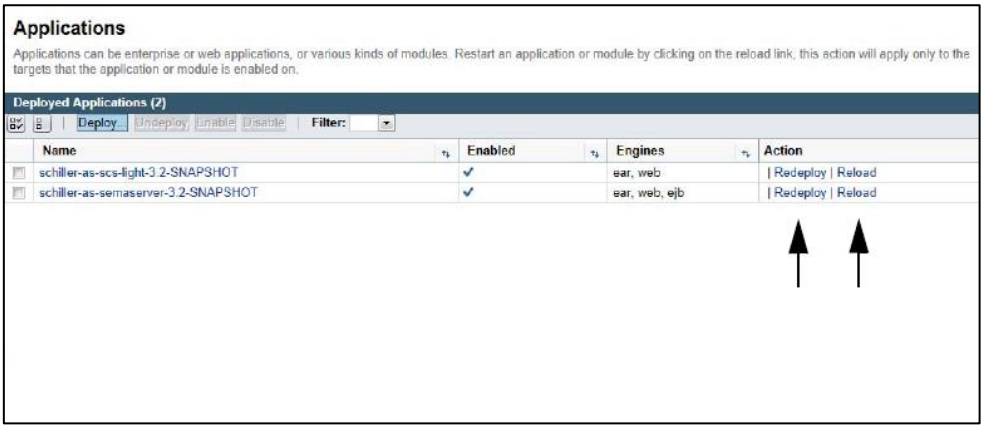
Slika 8.4 Prikaz prozora sa SEMA poslužitelj aplikacijom

Postupak je potrebno ponoviti da bi se rasporedile aplikacije vezane za komunikacijski poslužitelj. Odabirom „*List Deployed Applications*“ prikazuje se popis raspoređeni aplikacija (slika 8.5 i slika 8.6).



Slika 8.5 Prikaz početnog prozora

Uz svaku raspoređenu aplikaciju pod izborničkom grupom „*Action*“ administrator može odabrati opciju „*Reload*“ ukoliko je potrebno ponovno učitati aplikaciju ili opciju, „*Redeploy*“ ukoliko se ukaže potreba za ponovnim razmještanjem aplikacije (slika 8.6).

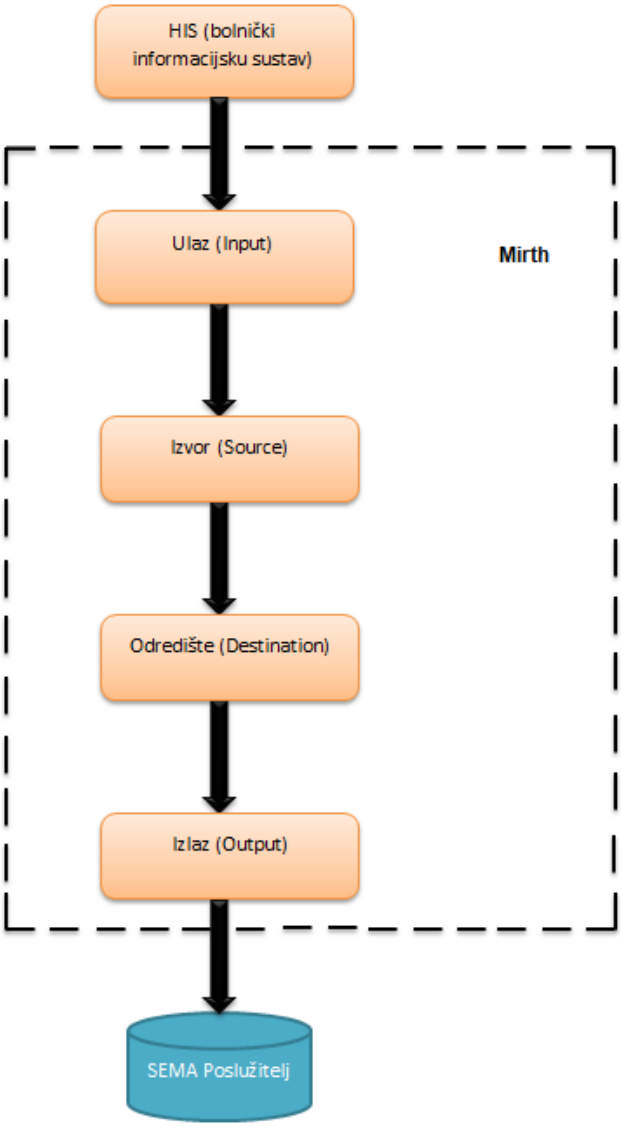


Slika 8.6 Prikaz prozora sa raspoređenim aplikacijama

9. Poslužitelj za povezivanje

Poslužitelj za povezivanje (Mirth) služi za integraciju vanjskih medicinskih sustava sa SEMA poslužiteljem. Poslužitelj (Mirth) omogućuje integraciju HL-7 i DICOM unutar medicine, te uključuje alate za dodatna testiranja, implementaciju i nadzor sučelja. Podržani su standardi za prijenos podataka od SEMA poslužitelja prema bolničkom informacijskom sustavu (HIS) i od HIS prema SEMA poslužitelju. Osim standarda vezanih uz mrežnu komunikaciju i aplikacijska rješenja - XML, mySQL, web servisi, koriste se i specijalizirani standardi uobičajeni u medicinskim sustavima - HL-7 i DICOM [8]

9.1. Osnovni tijek rada

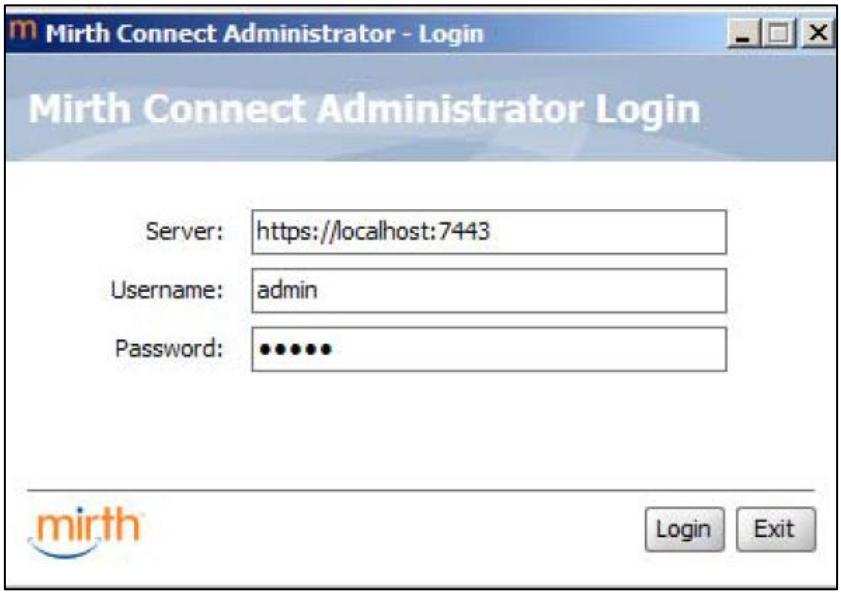


Slika 9.1 Prikaz osnovnog tijeka rada

Tijek rada (slika 9.1) prikazuje slanje podatka od bolničkog informacijskog sustava (engl. *HIS*) prema SEMA poslužitelju:

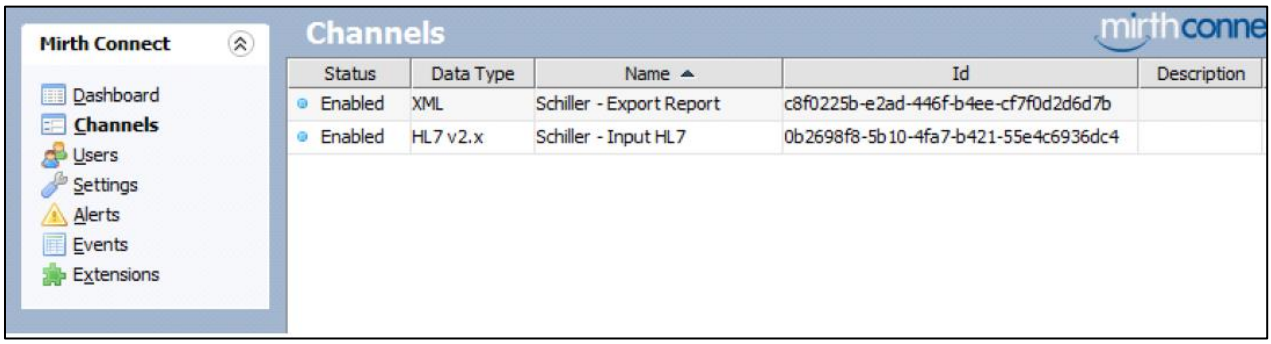
- Mirth primi podatak od bolničkog informacijskig sustava
- primljeni podatak se filtrira
- nakon filtracije je da se podatak šalje na izlaz
- podatak sa izlaza se šalje na SEMA poslužitelja

Isti je postupak kada se podatak šalje iz SEMA poslužitelja prema HIS sustavu. Na slici 9.2 je prikazano sučelje za prijavu administratora u Mirth poslužitelja. Nakon uspješne prijave administrator vrši nadzor i druge dozvoljene radnje.



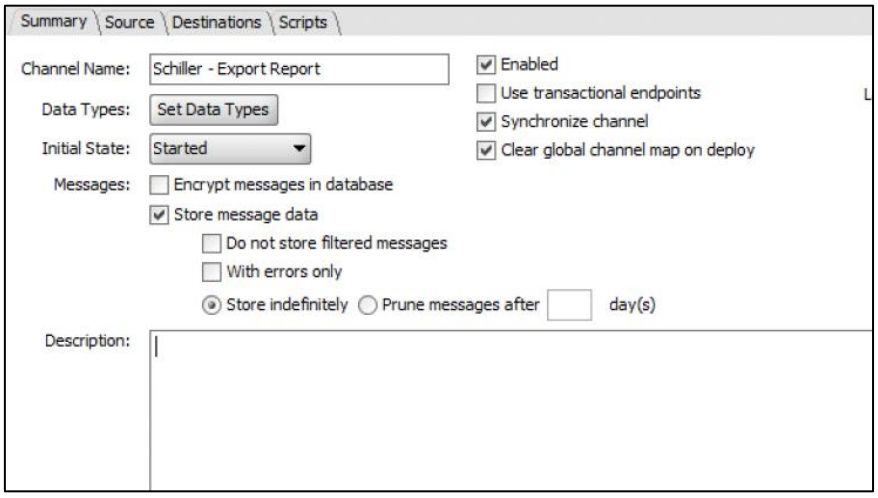
Slika 9.2 Prikaz prozora za prijavu

Mirth kanali predstavljaju „proces“ koji se izvodi na Mirth poslužitelju kad je kanal omogućen (*engl. enebled*) i raspoređen. Svaki kanal ima izvor i jedno ili više odredišta, dok između izvora i odredišta je postavljeno nekoliko filtera i transformatora. Svaki kanal mora imati jedinstveno ime.



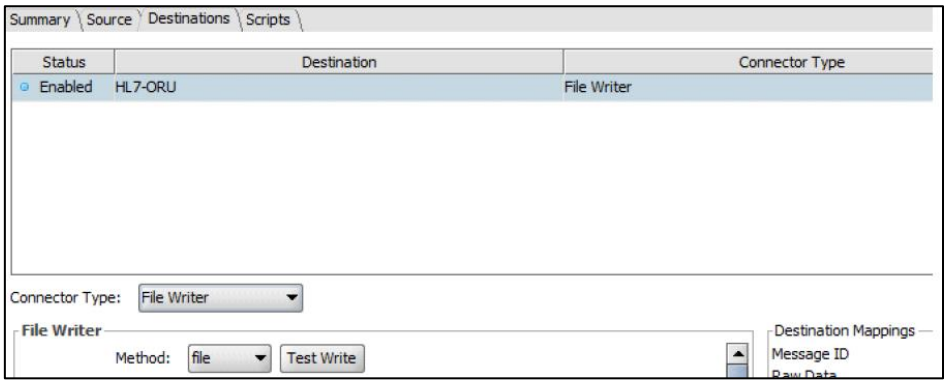
Slika 9.3 Prikaz prozora sa kanalima

Slika 9.3 prikazuje Mirth kanale koji su već raspoređeni i omogućeni. Odabirom „*Channels*“ u danom izborniku uređuje se novi Mirth kanal. Za uređivanje novog kanala postoje kartice „*Summary*“ , „*Source*“, *Destination*“ i „*Scripts*“ (slika 9.4).



Slika 9.4 Prikaz prozora za uređivanje kanala

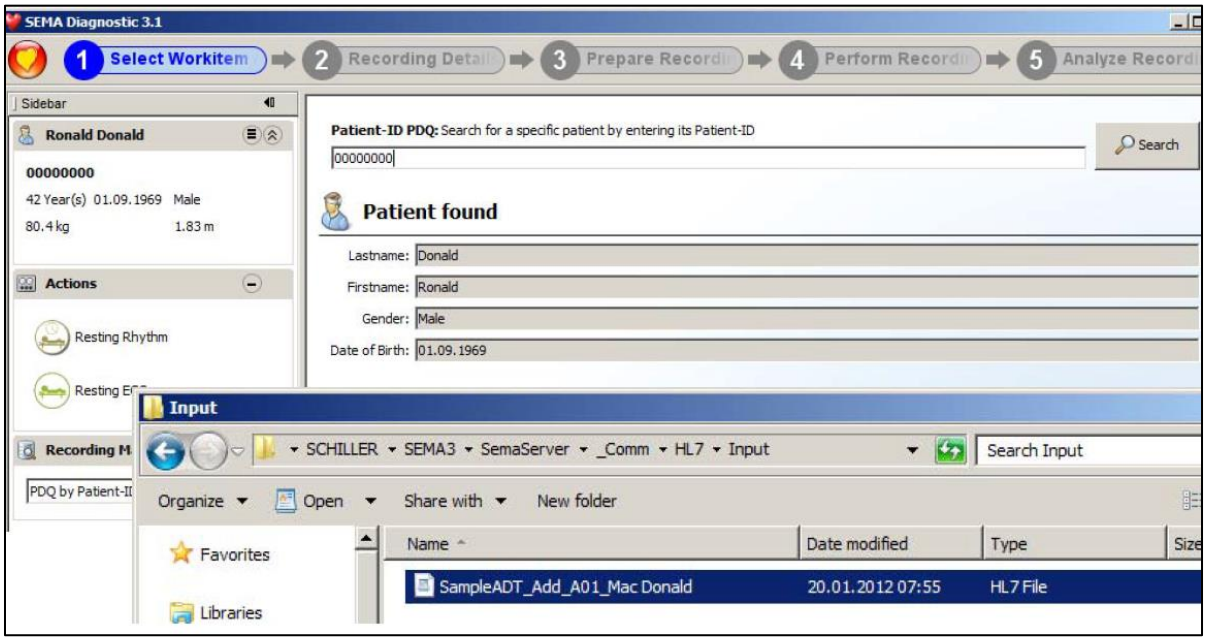
Nakon podešavanja svih potrebnih parametara status novog kanala se prikazuje kako je prikazano na slici 9.6. Administratoru je dostupna informacija o statusu kanala, destinaciji kanala i tipu konektora koji se koristi za komunikaciju. Detaljni parametri vezani uz podešavanja kanala između bolničkog informacijskog sustava i SEMA sustava su nam kao korisniku nedostupni, jer ih proizvođač sustava smatra poslovnom tajnom.



Slika 9.6 Prikaz prozora sa novo uređenim kanalom

Za potrebe provjere funkcionalnosti kanala administrator ima mogućnosti testiranja. Testiranje se provodi na način da se pošalje zahtjev za podacima o pacijentu sa sustava SEMA na bolnički informacijski sustav, te se čeka povratna informacija. Ukoliko se pojavi greška, tj. podaci o traženom pacijentu nisu stigli s bolničkog informacijskog sustava u sustav SEMA potrebno je ponoviti postupak raspoređivanja kanala. Važna napomena prije izvođenja testiranja je da u bolničkom informacijskom sustavu mora postojati pacijent za kojeg je poslan zahtjev.

Ako je zahtjev uspješno prikazan podaci su dostupni unutar sustava SEMA (slika 9.7). [10]



Slika 9.7 Prikaz prozora za testiranje kanala

9.2. Mirth filteri

Filteri se koriste za definiranje pravila bilo za izvor (engl. *source*), bilo za odredište (engl. *destination*). Filter izvora neće proslijediti poruku ili ju transformirati u drugi format ukoliko nisu ispoštovana njegova pravila. Takav postupak sprječava zagušenje veze sa nepotrebnim podacima ili neželjenim podacima. Kod odredišnog filtera ukoliko transformirani podatak ne zadovoljava pravila on se neće obrađivati. Filteri koji se koriste u ovom sustavu su *JavaScript* filteri.

9.3. Mirth transformeri

Transformeri služe za preobrazbu ulaznih podataka u bilo koju vrstu datoteka, te slanje istih na različita odredišta. U ovom sustavu se koriste jedna od tri vrste transformatora :

1. *Message Builder*
2. *Mapper*
3. *JavaScript*

Message Builder transformator radi na način da seli jednu vrijednost iz ulazne (dolazne) poruke na mjesto u odlaznu poruku i u međuvremenu izvodi pretvorbu.

Primjer :

- Message segment: `tmp['patient']['gender']`
- Mapping: `msg['PID']['PID.8']['PID.8.1'].toString()`
- Default value: `"Undefined"`
- String replacement: `"F" = female, "M" = male`

Mapper transformator radi na način da izvlači jednu vrijednost iz ulazne poruke na varijabli.

Primjer:

- Variable: `varRaceGroup`
- Mapping: `msg['PID']['PID.10']['PID.10.1'].toString()`
- Message segment: `tmp['patient']['ethnicity']`
- Mapping: `$('varRaceGroup')`

JavaScript transformeri može u jednom koraku obaviti preobrazbu opsežnih i složenih poruka, napraviti pretragu baze podataka za transformiranom vrijednošću, te izvesti mnoštvo drugih radnji nevezanih za pretvorbu poruke.
Primjer: Pretvarač datuma, pretvara datum rođenja i datum snimanja na međunarodno korišteni format „yyyyMMdd“ .

9.4. Mirth konektori

Konektori koje koristi Mirth isti su i za izvor (*engl. source*) i za odredište (*engl. destination*). Vrste konektora :

- *Channel Reader / Writer*
- *Database Reader / Writer*
- *FTP Reader / Writer*
- *File Reader / Writer*
- *HTTP Listener / Sender*
- *JMS Reader / Writer*
- *Java Script Reader / Writer*
- *LLP Listener / Sender*
- *SFTP Reader / Writer*
- *SOAP Listener / Sender*
- *TCP Listener / Sender*
- *Document Writer*
- *Email Sender*

9.5. Ranije verzije poslužitelja za povezivanje

Komunikacija sa bolničkim informacijskim sustavom (HIS) se u prijašnjim verzijama sustava SEMA obavljala pomoću GDT poslužitelja i GDT datoteka. Ova vrsta prijenosa podataka nije imala mogućnost pregleda signala EKG pretrage već su

bile poslane samo osnovne informacije vezane uz pretragu. Da bi se EKG uređaji povezani u sustav SEMA mogli uskladiti sa tim prohtjevima, proizvođač je razvio RST datoteku koja je omogućavala prepoznavanje kodova koji su označavali pojedini podatak.

ID	OPIS
8000	Tip pretrage
8100	Dužina snimke
8315	GDT-ID primatelja
8316	GDT-ID pošiljatelja
9218	GDT verzija
3000	Identifikacijski broj pacijenta
3101	Prezime pacijenta
3102	Ime pacijenta
3103	Datum rođenja pacijenta
3110	Spol pacijenta
3622	Visnina pacijenta
3623	Težina pacijenta
8432	Datum izvršene pretrage
8439	Vrijeme izvršene pretrage
8402	Tip pretrage
8470	Informacije vezane uz pretragu
6220	Interpretacija
6227	Komentar

Slika 9.8 Tablični prikaz popisa kodova korištenih za komunikaciju

Primjer GDT datoteke:

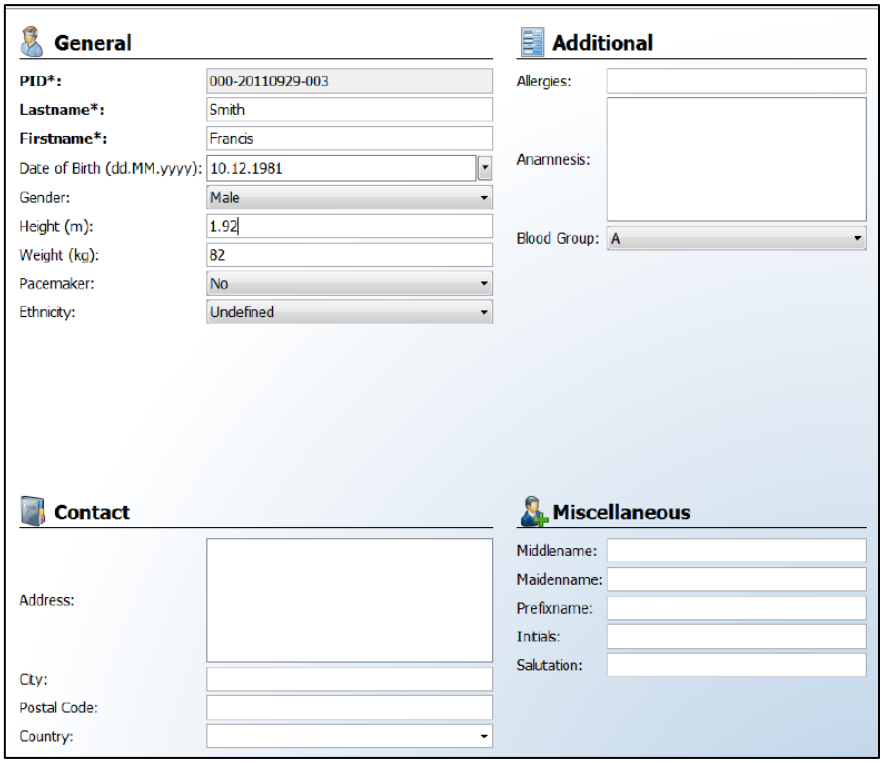
```
01380006310
014810000546
0138315EKG1
0138316SCH1
01492801.00
0133000010000
0163101PERIĆ
0153102PERO
017310316031940
01031101
0123622180
011362389
017843229032004
0158439145824
0158402ERGO01
017620029032004
0536220Pacijent doseže limit vježbe 50 W
0386220Max Puls 60 /43% / 140
```

Primjer prikazuje propisani format datoteka koji je sadržavao niz kodova (šifri) koji su se koristili za komunikaciju s bolničkim informacijskim sustavom, gdje su se pomoću protokola HL-7 mogli pročitati podaci vezani za pacijenta i pretragu. GDT datoteka je sadržavala vrlo malo važnih informacije vezanih za pretragu, tj. nije bilo moguće ništa zaključiti iz tih podataka ili postaviti dijagnozu. [11]

U današnjoj verziji SEMA sustava neke stvari su pojednostavljene korištenjem poslužitelja za povezivanje (Mirth). Iako su neki kodovi koriste i danas, jednostavnost je u tome što se danas šalju samo osnovni podaci (identifikacijski broj pacijenta, ime, prezime, godina rođenja) i u prilogu se šalje PDF dokument unutar kojeg se osim osnovnih podataka o pacijentu vidi EKG pretraga (vidi se EKG snimka) sa svim potrebnim podacima vezanim uz očitanje EKG signala, krvnog tlaka, srčanog ritma, trajanju pretrage, vremenu početka i završetka pretrage, dijagnoza liječnika, preporučeni sljedeći pregled itd. Primjenom novog poslužitelja ne samo da se olakšalo slanje podataka, već se šalje više podataka vezanih uz pacijenta tako da je moguće da i neki drugi liječnik pregleda EKG snimku, dok sa GDT datotekama to nije bilo moguće jer su rezultati pretrage bili poslani u brojčanom obliku, tako da npr. nije bilo moguće vidjeti točno vrijeme kada je srčani ritam dostigao maksimalnu vrijednost nego je ostala zabilježena samo ta maksimalna vrijednost.

10. Organizacija podataka

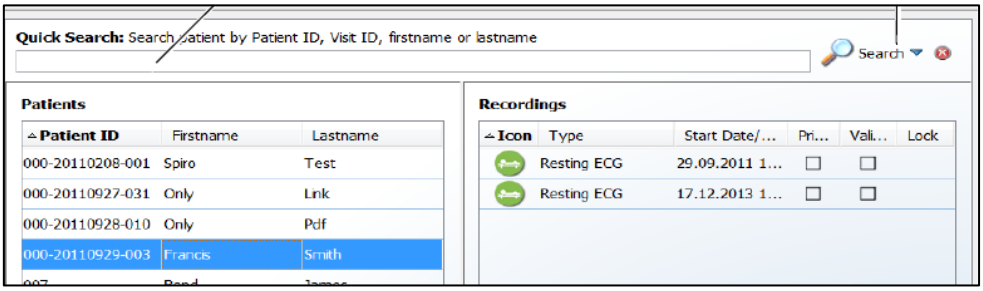
U ovom poglavlju daje se pregled osnovne organizacije podataka vidljivih krajnjim korisnicima - liječniku ili medicinskoj sestri. Zbog zatvorenosti sustava i ograničenih korisničkih ovlasti, precizna struktura baze podataka nije bila dostupna.



Slika 10.1 Prikaz prozora prilikom unosa novog pacijenta

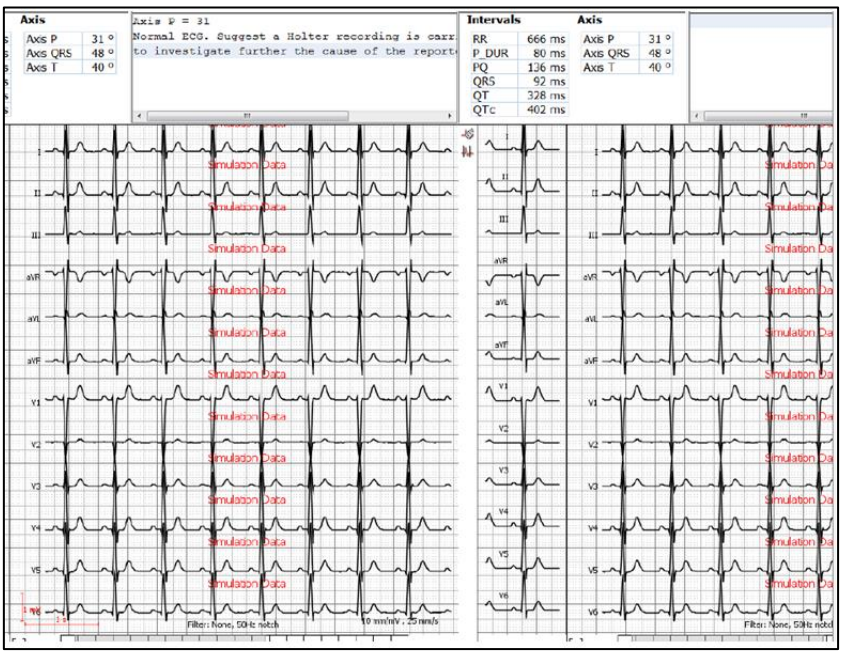
Slika 10.1 prikazuje koje podatke o pacijentu je potrebno unjeti prilikom spramanja novog pacijent u bazu podataka unutar sustava SEMA. Osim nekih osnovnih podataka poput imena, prezimena, adrese, imena grada, poštanskog broja, itd, postoje i podaci koji imaju važnost prilikom izvođenja pretraga. Ti podaci se odnose na datum rođenja, spol, visina, težina, da li pacijent ima *pacemaker*, krvna grupa, znane alergije, postavljene dijagnoze itd. Podaci poput dobne skupine, spola, indeksa tjelesne mase, znanih alergija, povijesti bolesti,tip krven grupe i sl. Potrebni su zbog dobivanja što točnije interpretacije dobivenog EKG signala. Međutim za ispravno funkcioniranje baze podataka najvažniji podatak je PID ili indentifikacijski broj podataka. Pošto je identifikacijski broj pacijenta jedinstven za svakog pacijenta unutar baze pojedinog korisnika olakšava samu pretragu baze podataka, te sprječava moguće greške i zabune vezne uz pretrage i analize EKG signala za pojedinog pacijenta. Iz prakse je poznato da postoji mogućnost da kod jednog korisnika (liječnika) postoji nekoliko pacijenta sa istim prezimenom ili imenom, a u rijetkim slučajevima dva različita pacijenta imaju isto ime i prezime. Da bi se spriječila moguća zabuna ili greška prilikom rada sa bazom podataka preporučljivo je pretraživati bazu podataka sa popisom pacijenta pomoću indentifikacijskog broj. Postoje i mogućnosti pretrage baze podataka prema prezimenu ili imenu pacijenta ili

prezimenu i imenu pacijenta. Pretraga baze podataka, tj traženje određenog pacijenta prikazano je na slici 10.2.



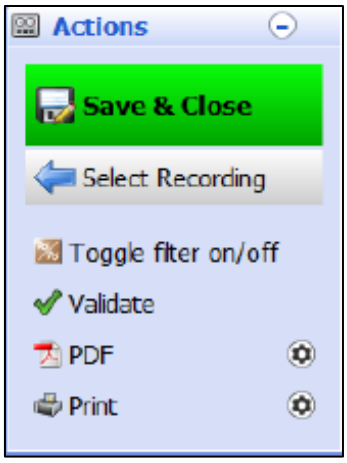
Slika 10.2 Prikaz prozora sa popisom na kojem se nalazi naš pacijenta i popis njegovih pretraga

Na slici 10.2 prikazan je postupak pretrage baze podataka gdje se u označeno polje upisuje indentifikacijski broj ili prezime ili ime ili prezime i ime pacijenta. Prilikom pronalaska pacijenta u bazi podataka njegovo ime se označi, te njegovim odabirom dobiva se popis odrađenih pretraga traženog pacijenta. U popisu pretraga vidljiv je simbol izvršene pretraga, naziv pretraga, te datum kada je pretraga izvršena. Odabirom jedna pretraga prikazuje nam se EKG signal dobiven izvođenjem pretrage (slika 10.3).



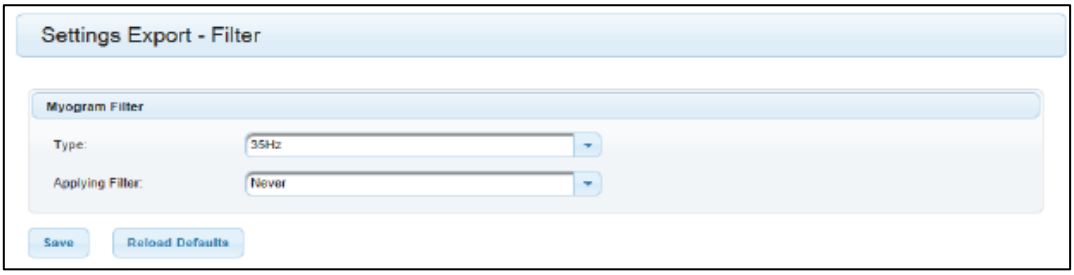
Slika 10.3 Prikaz izvedene pretrage

Na slici 10.3 je prikazan prozor sa rezultatima dobivenim EKG pretragom kojeg liječnici koriste za daljnju analizu rezultata, te za postavljanje dijagnoze. Postoje različite mogućnosti pregleda rezultata pretrage, npr. možemo povećati točno određeni dio EKG signala kojeg želimo detaljnije pregledati itd.



Slika 10.4 Prikaz izbornika

Na slici 10.4 vidljiv je izbornik koji je dostupan korisniku, gdje se može odabrati željeni način pohrane rezultata pretrage. Odabirom mogućnosti „*Save & Close*“ korisnik sprema komentare ili oznake koje su rađene na snimci, te zatvara pregled izvršene pretrage. Odabirom mogućnosti „*Select Recording*“ korisnik se vraća na popis izvršenih pretraga bez mogućnosti za spremanjem komentara ili zabilješki rađenih na snimci pretrage. Odabirom „*Toggie Filter on/off*“ korisniku je dana mogućnost da odredi jačinu filtera koji se koristi za „peglanje signala“ tj. da se dobije što „čišći“ EKG signal bez smetnji. Odabirlom „*Validate*“ korisnik označuje da je izvršena pretraga pregledana, te da je dobiveni signal zadovoljavajući, jer u rijetkim slučajevima se može dogoditi da izvršena pretraga može biti ne upotrebljiva zbog nastalog kvara na EKG uređaju i računalu koje se koristi za pregled podataka ili zbog prekida Internet veze prilikom slanja podataka s EKG uređaja na SEMA poslužitelja. Odabirom mogućnosti „*PDF*“ pretraga se ispisuje kao PDF dokument, dok odabirom „*Print*“ pretraga se ispisuje na pisaču. Za ispis rezultata u PDF dokumenta mogu se postavljati određene postavke: naziv dokumenta, redoslijed ispisa signala EKG-a (da li želimo da nam se ispišu svih 12 izvoda, ili samo 6 izvoda ili samo 3 izvoda), tip i boja mreže na podlozi, te boja podloge (najčešće crvena). Također se može postaviti filter frekvencija kojima se dodatno „pročisti“ dobiveni EKG signal od mogućih smetnji pošto se EKG mjeri u milivoltima.



Slika 10.5 Prikaz prozora za odabir filtera

Ovaj dio sustava namjenjen je korisniku (liječniku) gdje si on po vlastitoj želji i potrebi može filtrirati i prilagođavati ispis podataka za pojedinog pacijenta. Iz svega toga je

vidljivo da je SEMA baza podataka vrlo jednostavno sastavljena, jer je cilj ovog sustava da se što brže dođe do željenih podataka. Kupnjom SEMA licence korisnik dobija pristup svojoj bazi podataka na SEMA poslužitelju. Takav koncept upravljanja podacima naziva se klijent-poslužitelj sustavi.

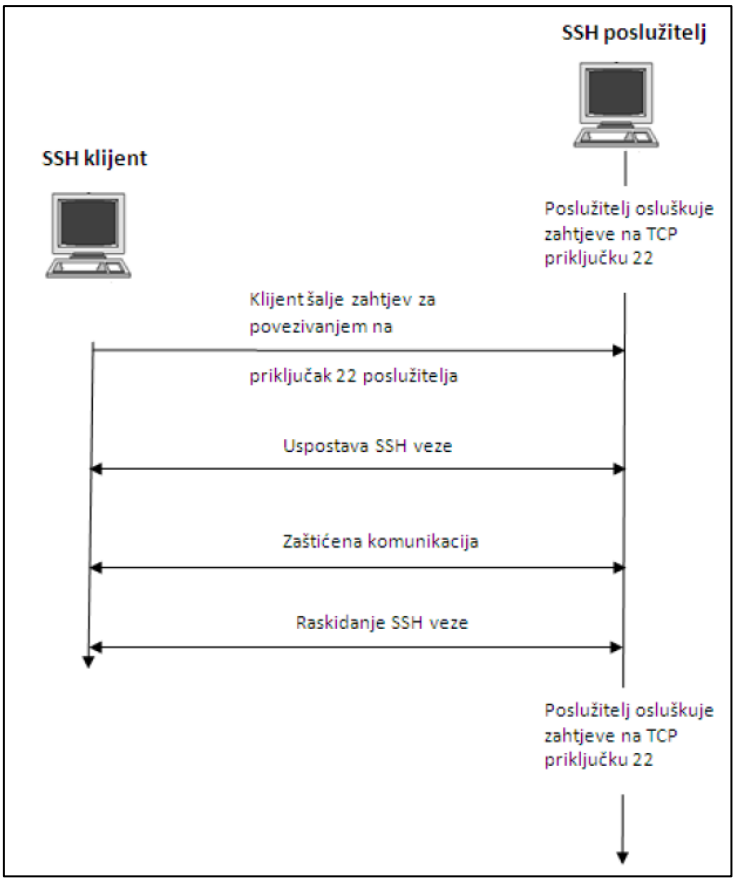
U suštini današnji oblik centraliziranih sustava su klijent-poslužitelj sustavi u kojima poslužitelj zadovoljava zahtjeve generirane od strane klijenta. [9]

Poslužiteljski sustav možemo podijeliti na:

a) Poslužitelj transakcija (*engl. transaction server*) koji nudi sučelje kojim klijenti mogu poslati zahtjev za izvršavanje neke akcije
b) Poslužitelj podataka (*engl. date server*) koji čuva podatke, a kojima pristupaju klijenti

11. Komunikacija putem Interneta

Internet predstavlja nesigurnu mrežu,, pa se komunikacija unutar SEMA sustava koristi kriptografski mrežni protokol SSH (engl. *Secure Shell*). Ovaj mrežni protokol omogućuje siguran protok povjerljivih podataka kroz nesigurnu mrežu, a to se postiže pomoću kriptografije javnim ključem. Ova vrsta kriptografije se temelji na paru komplementiranih ključeva od kojih je jedan „javni“ , a drugi „tajni“ (privatni) ključ. Javni ključ se slobodno prenosi ili distribuira dok se tajni ključ čuva i on je dostupan samo korisniku. Asimetričnim algoritmima se obavlja enkripcija i dekripcija i to na način da jedan ključ se koristi za kriptiranje, a drugi ključ se koristi isljkučivo za dekriptiranje. U SEMA sustavu javni ključ se koristi za kriptiranje, dok se dekriptiranje obavlja tajnim ključem. Na taj način poslani podaci su zaštićeni jer samo korisnik sa tajnim ključem ih može dekriptirati. Provjera indentiteta korisnika se obavlja pomoću digitalnih certifikata. Proizvođač SEMA sustava izdaje digitalni certifikat kojim se jamči veza između javnog ključa i njegovog korisnika. Certifikati sadrže indentifikator i javni ključ korisnika, te digitalni popis indentifikacijskog centra. SSH se temelji na modelu klijent – poslužitelj, što znači da se komunikacija odvija između dvije različite strane. Na jednoj strani je poslužitelj koji osluškuje zahtjeve na unaprijed zadanim mrežnim vratima (engl. *Port*) transportnog sloja (vrata TCP protokola), a klijent po potrebi šalje zahtjeve poslužitelju. [10]



Slika 11.1 Prikaz komunikacije između klijenta i poslužitelja

Na slici 11.1 je prikazan primjer kada SSH poslužitelj osluškuje zahtjeve klijenta na vratima 22. [11]

Klijent pošalje zahtjev za komunikacijom (povezivanjem) sa vratima 22 poslužitelja, nakon čega se uspostavi SSH veza, te slijedi zaštićena komunikacija. Nakon raskida SSH veze poslužitelj dalje osluškuje zahtjeve na TCP vratima 22. Za uspostavu komunikacije i samu komunikaciju u SSH protokolu koriste se tri sloja:

1. Transportni sloj (engl. *Transport Layer Protocol*)
2. Autentifikacijski sloj (engl. *Authentication Protocol*)
3. Spojni sloj (engl. *Connection Protocol*

11.1. Transportni sloj

Ovaj sloj SSH protokola osigurava enkripciju i zaštitu integriteta podataka, te autentifikaciju poslužitelja. Također omogućeno je i sažimanje (kompresija) podataka, u SEMA sustavu podaci se sažimaju u ZIP format, što omogućuje brzi i jednostavniji prijenos. Za razmjenu podataka nakon uspostave SSH veze na transportnom sloju se koristi binarni paketni protokol (engl. *Binary Pacage Protocol*). U ovom protokolu komunikacija se odvija pomoću posebno organiziranih nizova bitova koji predstavljaju pakete. Podaci se nadopunjuju do neke pogodne duljine, koja je često povezana sa algoritmom kriptiranja koji se koristi. U SEMA sustavu kriptiraju se blokovi od 1024 bita.

duljina paketa	duljina dopune	podaci	dopuna	MAC

Slika 11.2 Prikaz paketa

Na početak paketa zapisuje se duljina dopune , te ukupna duljina paketa koja uključuje zbroj duljine podataka, dopune i duljinu dopune. Ovi podaci se kriptiraju prije slanja. MAC vrijednost se izračunava i ona osigurava integritet poslanih podataka, te se ona ne kriptira.

11.2. Autentifikacijski sloj

Komunikacija na tom sloju se uspostavlja nakon što je uspostavljena komunikacija na transportnom sloju. Autentifikacijski sloj omogućuje provjeru indentiteta klijenta na poslužitelju , a to je moguće napraviti na više načina:

1. PKI (engl. *Public Key Infrastructure*) metode autentifikacije koje se temelje na digitalnim potpisima i asimetričnim kriptografskim algoritmima, te na provjeri certifikata
2. Putem lozinke koja se kriptirana šalje SSH kanalom
3. Autentifikacija zasnovana na provjeri klijanta u bazi računala kojima je dopuštena autentifikacija, a koja se nalaze na poslužitelju.

Ovim slojom ostvaruje se jedinstveni SSH komunikacijski kanal.

11.3. Spojni sloj

Na ovom sloju ostvaruju se udaljene prijave korisnika , udaljeno izvođenje naredbi i povezivanje svih veza u jedan kriptirani kanal. Na nižim razinama (slojevima) SSH arhikteture kanali se prenose preko jedne veze, dok u spojnom sloju virtualno se raspolaže sa proizvoljnim brojem kanala koji se međusobno razlikuju pomoću indentifikatora. Spojni sloj je najviša razina SSH arhikteture sa kojim je korisnik u najizravnijem i direktnom dodiru.

Iz svega je vidljivo da je SSH protokol aplikacijske razine osigurava tajnost i integritet podataka koji se razmjenjuju između dva odredišna korisnika (računala). Također važno je napomenuti da SSH pruža određenu razinu zaštite prilikom korištenja Interneta, ali ne i potpunu, pošto SSH ne provjerava podatke koji se šalju i pretpostavlja pouzdanost krajnjih korisnika.

11.4. Dopuna SSH sigurnosti

TLS je sigurnosni protokol kojim se omogućuje zaštitna komunikacija na Internetu. Nalazi se na transportnom sloju mrežne komunikacije, dok je SSH aplikacijski protokol i on je prethodnik TLS protokola.

TLS se odvija u tri osnovne faze:

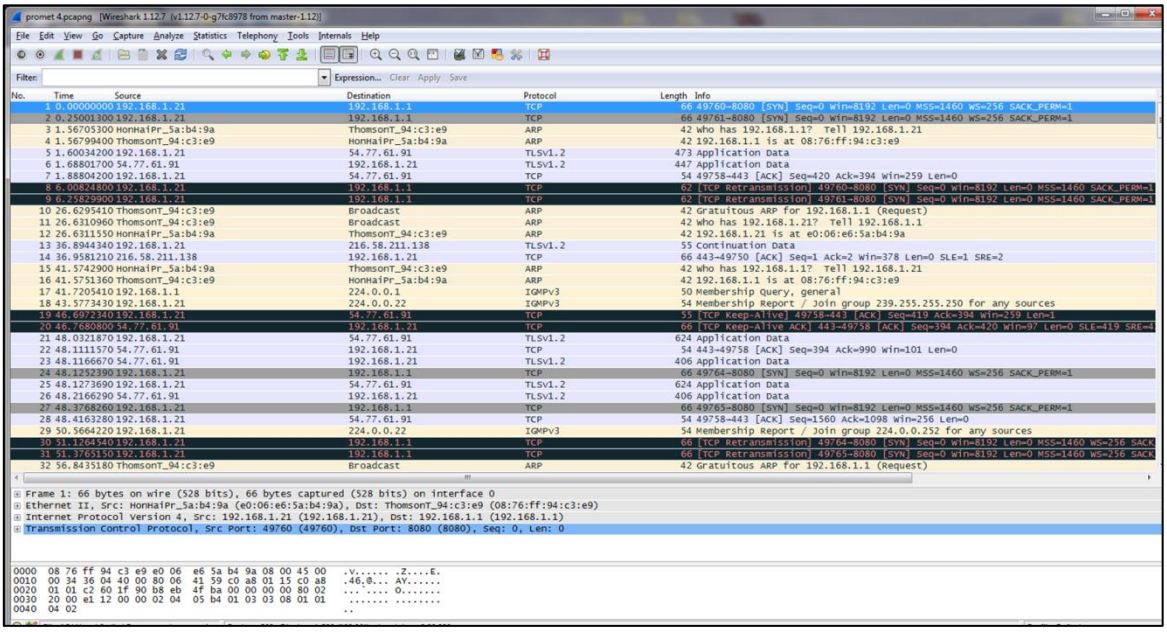
1. dogovaranje algoritma
2. razmjena ključa i autentifikacija
3. simetrična enkripcija poruka i provjera autentičnosti i integriteta.

Za razliku od SSH protokola, TLS ne traži nužno autentifikaciju poslužitelja. Moguće je uspostaviti TLS vezu između potpuno anonimnih korisnika. TLS zahtjeva PKI autentifikaciju x.509 certifikatima, dok SSH podržava takvu autentifikaciju kao mogućnosti. TLS ne podržava usluge poput udaljenog pokretanja programa, tuneliranja drugih protokola, veza i sl. Dostupan je u besplatnim OpenTLS i NNS bibliotekama.

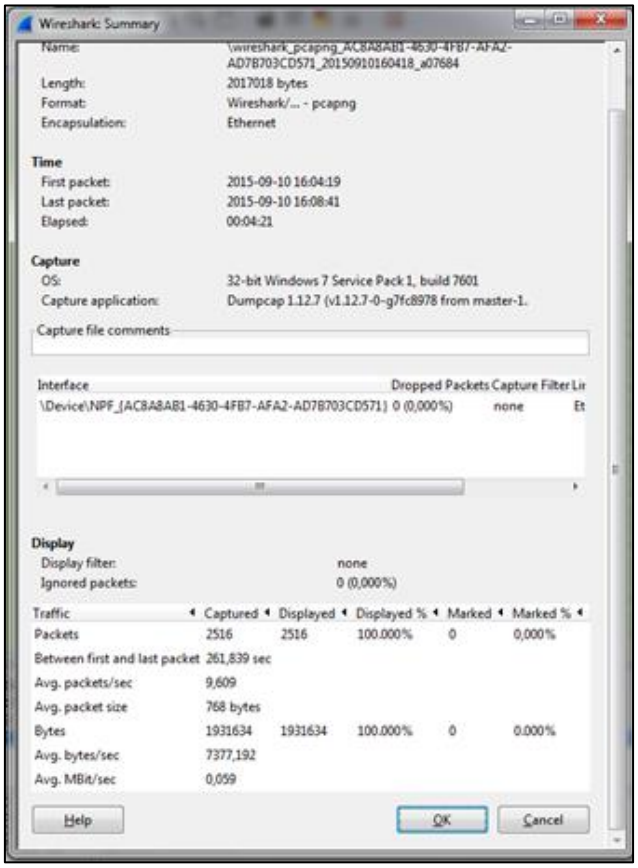
11.5. Snimanje prometa

U ovom poglavlju prikazana je snimljena komunikacija između korisnika i poslužitelja. Za postupak snimanja prometa korišten Wireshark program. Wireshark je programski alat koji se koristi za analizu mreže, tj. mrežnih protokola, a radi na principu da snimi protok paketa u realnom vremenu koji se šalju unutar neke mreže. On je dostupan na operacijskim sustavima i svim platformama. Nakon prijave u SEMA sustav i odabira pacijenta iz baze podataka, odabrana je opcija za ispis

rezultata EKG pretrage u PDF formatu. Cijelo vrijeme bio je uključen programski alat Wireshark koji je snimio promet na mreži.



Slika 11.7 Prikaz snimljenog prometa



Slika 11.8 Prikaz podataka o ukupnom snimljenom prometu

Sa slike 11.8 vidljiv je sažetak koliko je paketa poslano tijekom ovog postupka i da su svi paketi uspješno poslani. Adresa korisnika u našem slučaju je 192.168.1.21, dok je adresa SEMA poslužitelja u našem slučaju 192.168.1.1. Snimanje je obavljeno u novijoj verziji SEMA sustava za koju nam nisu dostupne tehničke informacije, pa na temelju snimljenog prometa možemo zaključiti da se koriste sigurnosni komunikacijski protokoli TLS v1.2, što nam onemogućuje analizu konkretnog prometa, ali istovremeno nam sugerira da najvjerojatnije nova verzija sustava ne koristi SSH kao stara. U komunikacije se pojavljuje dodatna IP adresa koja se vjerojatno odnosi na samo sjedište proizvođača sustava, pošto nam je poznato da se podaci šalju na poslužitelj proizvođača.Također je vidljivo da se za komunikaciju koristi protokol IPv4. Kako je već prije objašnjeno SEMA poslužitelj koristi vrata (port) 8080, podešen tijekom instalacije SEMA sustava.

12. Zaključak

U završnom radu dan je uvid u sustav SEMA švicarskog proizvođača EKG uređaja Schiller. Sustav SEMA je namijenjen za umrežavanje EKG uređaja i računalno upravljanje EKG dijagnostičkim postupkom, te se sastoji od tri osnovne verzije (SEMA Solo, SEMA Diagnostic, SEMA Workstation) od kojih svaka nudi različite mogućnosti za upravljanjem. Funkcionalnost sustava je moguća pomoću standardnih podsustava: poslužitelj baze podataka (MySQL), Java programskog okruženja (JDK/JRE) i aplikacijskog poslužitelja (Glassfish), te standardnih mrežnih protokola i specijaliziranih mrežinih protokola (HL-7 , DIACOM). Organizacija podataka, omogućava krajnjem korisniku (liječniku) brz i efikasan rad, te sprječava gubitak važnih podataka (EKG snimka). Za mrežnu komunikaciju unutar sustava SEMA koriste se standardni protokoli (IPv4, TCP), dok za sigurnu komunikaciju koriste se rješenja bazirana na TLS protokolu. Iz svega navedenog mogu zaključiti da sustav SEMA predstavlja jedno inovativno IT rješenje, čijim korištenjem se može poboljšati kvaliteta dijagnostike i samog liječenja pacijenta, dok s druge strane ubrzava rad i efikasnost medicinskoga osoblja.

13. Literatura

[1] http://www.wikipedia.org, dostupno 29.06.2015.

[2] http://www.hl7.org, dostupno 29.06.2015.

[3] http://www.diacom.technology.com, dostupno 29.06.2015.

[4] http://www.iana.org, dostupno 29.06.2015.

[5] http://www.securityfocus.com, dostupno 29.06.2015.

[6] Test verzija SEMA sustava, Baar, Švicarska, 2014

[7] http://glassfish.java.net, dostupno 29.06.2015.

[8] http://www.mirthcorp.com, dostupno 29.06.2015.

[9] Robert Manager, Baze Podataka, skripta, Zagreb, 2008

[10] Korisnička uputstva SEMA sustava, skripta, Baar, Švicarska, 2014.