Arhitekturni izzivi razvoja rešitve Connected mHealth

Damjan Kovač, Sebastjan Juhart, Tina Maček, Matevž Klevže, Saša Saje Wang

Mikropis Holding d.o.o., Žalec, Slovenija
damjan.kovac@mikropis.si, sebastjan.juhart@mikropis.si, tina.macek@24alife.com, matevz.klevze@24alife.com, sasa.sajewang@mikropis.com

Sinopsis Izraz mHealth (m-zdravje) se nanaša na medicinske in javnozdravstvene prakse, ki se izvajajo in so podprte z mobilnimi napravami. Aplikacije mHealth vključujejo uporabo mobilnih naprav za zbiranje zdravstvenih podatkov, dostavo in izmenjavo zdravstvenih informacij za zdravnike, raziskovalce in paciente, spremljanje bolnika, neposredno zagotavljanje oskrbe (prek mobilne telemedicine), pa tudi usposabljanje in sodelovanje zdravstvenih delavcev. mHealth rešitve so prisotne že nekaj časa, vendar se je povpraševanje po njih enormno povečalo v času pandemije COVID-19. Connected mHealth, rešitev, ki smo jo razvili v podjetju Mikropis je ena izmed tovrstnih mHealth rešitev, ki se osredotoča predvsem na rehabilitacijo na daljavo. Namen rešitve je zagotoviti kvalitetno fizioterapevtsko obravnavo in obravnavo delovne terapije ter ju prenesti v izvajanje na pacientovem domu. V želji, da bi resnično ustvarili edinstveno rešitev na področju rehabilitacije, smo v razvoj produkta vključili strokovnjake iz različnih področij tehnologij, medicine in zdravja. Naš cilj je bil razviti enostavno in uporabno platformo, ki je na eni strani namenjena različnim strokovnjakom v zdravstvenih in rehabilitacijskih centrih, pri ustvarjanju in dodeljevanju individualiziranih rehabilitacijskih programov svojim pacientom, na drugi strani pa izboljšani uporabniški izkušnji, večji motivaciji in uspešnejši rehabilitaciji pacientov. Pri razvijanju tovrstne rešitve smo izbrali komponente, programski jezik in uporabniški vmesnik, ki omogoča varno, zanesljivo in enostavno uporabo tako za fizioterapevte, ki planirajo rehabilitacijske plane pacientom, kot tudi za paciente, ki planirane rehabilitacijske plane nato izvajajo preko mobilne aplikacije.

Ključne besede:
mHeatlh,
varnost podatkov
Keycloak SSO
IBM CDN

Univerzitetna založba Univerze v Mariboru
ISBN 978-961-286-639-6
DOI https://doi.org/10.18690/um.feri.10.2022.19

1 Uvod

Zdravstvene ustanove se srečujejo z vedno večjimi težavami pri zagotavljanju kakovostne in cenovno sprejemljive rehabilitacije, saj se število prebivalstva, ki se srečuje z eno od oblik zmanjšane zmožnosti gibanja ali celo invalidnosti na letni ravni povečuje. Zaradi povečanega povpraševanja in potrebi po rehabilitaciji so se začeli razvijati sistemi eHealth (dostop do informacij na spletnih portalih), TeleHealth (termin za vse zdravstvene storitve, ki se izvajajo s pomočjo informacijske in komunikacijske tehnologije), Telemedicina (raba sodobne informacijske tehnologije, z namenom zagotavljanja zdravstvenih storitev pacientom na daljavo), mHealth (kjer uporabnik prejme na pametni telefon personalizirano informacijo oz vodeno vadbo, preko katere je voden med zdravljenjem, lahko pa se uporabi tudi kot nadaljevanje zdravljenja, ko uporabnik zapusti rehabilitacijski center in nadaljuje rehabilitacijo doma). Telemedicina in mHealth storitve zajemajo zgodnjo oziroma podaljšano rehabilitacijsko obravnavo in terapevtsko vadbo, katero pacienti izvajajo v bližnji zdravstveni ustanovi ali kar doma. mHealth je zaradi široke dostopnosti in razširjenosti mobilnih naprav optimalna rešitev, ki omogoča oskrbo in storitve širokemu spektru prebivalstva. V podjetju Mikropis, skupaj s kliniko Mayo Clinic razvijamo rešitve na področju preventive. Zaradi vse večje potrebe po naprednih in mobilnih rešitvah na področju rehabilitacije pa smo se skupaj lotili razvoja mHealth rešitve Connected mHealth – rehabilitacija na daljavo. Pri implementaciji rešitve smo morali poiskati in rešiti številne vsebinske in programerske izzive, ki so podrobneje predstavljeni v nadaljevanju.

2 Izzivi razvoja rešitve Connected mHealth

2.1. Zasebnost in varnost podatkov

Cilj razvoja rešitve Connected mHealth je bil razviti enostavno in uporabno platformo, ki je na eni strani namenjena različnim strokovnjakom v zdravstvenih in rehabilitacijskih centrih, pri ustvarjanju in dodeljevanju individualiziranih rehabilitacijskih programov svojim pacientom, na drugi strani pa izboljšani uporabniški izkušnji, večji dostopnosti, motivaciji in uspešnejši rehabilitaciji pacientov.

Glede na cilj rešitve, Connected mHealth sodi med rešitve namenjene uporabi za zdravstvene oziroma rehabilitacijske namene, v obliki mobilne aplikacije in spletnega portala, ki morata biti razvita tako, da je izmenjava podatkov med pacienti (uporabniki) in strokovnjaki v zdravstvenih in rehabilitacijskih centrih popolnoma zanesljiva in varna. To je bila glavna stvar, ki smo jo imeli v mislih pri sami zasnovi in implementaciji produkta.

Prvi izziv s katerim smo se soočili je bil torej točnost, zasebnost in varnost podatkov ter implementacija dostopov za različne vloge, pri čemer smo upoštevali previdnostna načela, ki zagotavljajo, da ne bo škode tako za strokovnjaka, kot za pacienta – oba ključna uporabnika rešitve. Dostop do podatkov pacienta je tako omogočen le strokovnjakom in nikomur drugemu, niti npr. administrativnim osebam, ki uporabnike t.i. paciente naročajo na preglede ipd. Ti imajo le omejen dostop, ki ga potrebujejo za nemoteno delo pri kreiranju novih pacientov, deaktivaciji ipd.

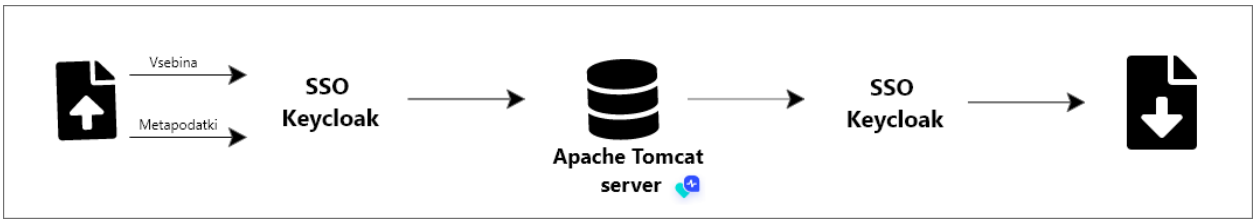
Znotraj rešitve Connected mHealth ima strokovnjak med drugim tudi možnost, da na svojega pacienta pripne razne priloge (dokumente) ter si tako ustvari "zdravstveni karton aktivnosti" pacienta.

Za zagotavljanje varnosti teh podatkov smo razvili lastnem sistem shranjevanja in hranjenja datotek (angl. File storage), ki je opremljen s pravicami nalaganja in dostopanja. Glede na različne vloge, ki so integrirane s SSO sistemom, se razlikujejo pravice in dostopi do naloženih podatkov in datotek. Zaenkrat imamo implementirane štiri različne vloge: "public", "company", "corporation" in "private". Kadar se gre za zdravstveno kartoteko uporabnika govorimo o "private", kadar se gre za shranjevanje novih vaj znotraj ene organizacije, ki jih kreirajo in naložijo strokovnjaki govorimo o "company" ali "corporation". Odvisno od velikosti naročnika in njihovih želja. Kadar je na voljo vsem uporabnikom rešitve pa govorimo o "public".

Vsi podatki oziroma dokumenti, ki jih strokovnjaki naložijo preko Connected mHealth rešitve so avtomatsko kriptirani in se servirajo dekriptirano, preko SSO tokena. Kriptirani so tako, da so zunaj rešitve neuporabni. V kolikor je SSO token potekel oziroma je neveljaven pomeni, da uporabnik do datotek ne more dostopati. Vsaka datoteka je ob kriptiranju sestavljena iz dveh delov – iz vsebine in iz meta podatkov, ki sta shranjena ločeno ter se ob vpogledu nato sestavita nazaj v eno datoteko.

V metapodatkih datoteke se beleži kompleten »audit log« datoteke v katerem so navedene vse spremembe in podatki o datoteki. Ti so:

- lastnik oziroma avtor datoteke,
- datum in čas nastanka,
- vrsta datoteke,
- pravice in vloge ki lahko dostopajo do datoteke,
- vsi ogledi datoteke (datum in čas) ter morebitne spremembe (datum in čas).



Slika 1: Nalaganje, enkriptiranje in dekriptiranje datoteke.
Vir: lasten.

2.2. »Audit log« oziroma revizijska sled

Zaradi podatkov, ki jih lahko strokovnjaki znotraj rešitve shranijo na profilu uporabnika (npr. zdravstveni izvid pacienta) in zaradi splošne zagotovitve ustrezne zasebnosti in varnosti osebnih podatkov smo znotraj rešitve Connected mHealth imlementirali tudi »audit log« oziroma revizijsko sled.

»Revizijska sled je dnevnik z zapisi o operacijah nad poslovnimi podatki. Je nespremenljiva sled oziroma niz podatkov, ki se je zgodila v informacijskem sistemu, z natančnim časovnim zapisom v obliki dnevniškega zapisa, ki omogoča natančni pregled vseh zapisov povezanih z vsemi poslovnimi dogodki in vsemi shranjenimi informacijami od nastanka podatka ali informacije dalje do trenutnega stanja. Omogoča ugotavljanje skladnosti in zakonitosti. Pomembno je, da beleži kdo, kdaj, do kakšnih podatkov je dostopal in kakšno operacijo je izvedel nad določenimi shranjenimi podatki. S tem je omogočen naknaden vpogled do vseh podatkov do katerih so dostopali uporabniki in vpogled v spremembe, ki so jih s svojimi aktivnostmi ustvarili. Revizijska sled mora biti nespremenjena, pregledna, sporočilna, dokumentirana in zaupna.«[8]

Implementirali smo torej sistem, ki zabeleži vsak vpogled strokovnjaka v podatke uporabnika (pacienta) in beleži vsako spremembo, ter tako zagotavlja večjo zasebnost in varnost pacienta oziroma njegovih osebnih podatkov. Za spremljanje vpogledov in delovanje »Audit loga« oziroma revizijske sledi je omogočeno filtriranje po datumu in vrsti dogodka ter vpogled v aktivnosti posameznega strokovnjaka.

Za vsak dogodek se zapišejo naslednji podatki:

- datum in čas,
- ime strokovnjaka,
- in opis dogodka.

Beležijo se naslednji dogodki:

- vpogled v podatke oziroma v profil uporabnika (pacienta),
- sprememba osebnih podatkov uporabnika (pacienta),
    - sprememba imena,
    - sprememba priimka,
    - sprememba kontaktnih podatkov,
- sprememba BIO podatkov,
    - sprememba spola,
    - sprememba datuma rojstva,
    - sprememba podatka teže,
    - sprememba podatka višine,
    - sprememba podatka max. heart rate,
    - sprememba podatka utripa v mirovanju,
    - sprememba naziva diagnoze,
    - sprememba opisa diagnoze,
    - dodana priloga,
    - odstranjena priloga,
    - vpogled v prilogo oziroma priloženo datoteko,
- sprememba plana,
    - sprememba naziva plana,
    - dodan nov plan,
    - odstranjen plan,
    - sprememba plana,
    - dodan nov protokol,
    - odstranjen protokol,
    - sprememba protokola,
- sprememba dodeljenega strokovnjaka,
    - dodeljen strokovnjak,
    - odstranjen strokovnjak,
- sprememba statusa skupin,
    - dodan v skupino,
    - odstranjen iz skupine.

3 Enotna prijava in deljenje podatkov z obstoječimi sistemi

Naslednji izziv nam je predstavljala enotna prijava in deljenje podatkov z obstoječimi sistemi. Naše obstoječe stranke, med katerimi je tudi klinika Mayo Clinic, s katero smo se tudi lotili razvoja rešitve, namreč že uporabljajo naše rešitve na področju preventive, ob tem pa tudi druge zunanje programe oziroma ponudnike, ki so si jih zaželeli v sklopu razvoja rešitve povezati in pacientom, ter zdravstvenemu osebju omogočiti enotno prijavo. Izgradnja novega sistema za overitev in pooblastitev, ki bi zadovoljila vsem zahtevam po povezovanju različnih produktov, sistemov in znanj bi nam predstavljala veliko časovno in stroškovno oviro, zato smo se lotili iskanja najprimernejše rešitve.

Po preučitvi kar nekaj rešitev smo se odločili za uporabo Keycloak SSO strežnika, ki omogoča enotno prijavo (IdP) z upravljanjem identitete in upravljanjem dostopa za sodobne aplikacije in storitve. Rešitev ponuja enkraten vpis v sistem, kar omogoča, da se uporabnik vpiše z enim ID-jem in geslom, ki velja v več medsebojno povezanih neodvisnih sistemih. Vsebuje nadzorno konzolo za upravljanje z domenami in za vsako domeno je mogoče nastaviti odjemalce, vloge, uporabnike in skupine. Keycloak SSO strežnik je napisan v Javi in privzeto podpira protokole federacije identitete SAML v2 in OpenID Connect (OIDC) / OAuth2. Je odprtokodni sistem, ki ima Licenco Apache.

Prednosti Keycloack SSO, ki so nas prepričale:

- enotna prijava (angl. Single-sign On),
- podpora za standardne protokole (OpenID Connect, OAuth 2.0 and SAML 2.0),
- centralizirano upravljanje,
- omogoča varne aplikacije in storitve,
- LDAP in Active Directory omogoča povezave z obstoječimi uporabniškimi imeni,
- možna "družabna prijava" (angl. Social Login),
- posredovanje identitete preko OpenID Connect or SAML 2.0 IdPs,
- visoka zmogljivost: lightweight, fast and scalable,
- preproste teme za izvedbo,
- močno preverjanje pristnosti z izvorno enkratno kodo (OTP) prek FreeOTP ali Google Authenticator,
- prilagajanje politike gesel,
- odprte možnosti razširljivosti: uporabniška baza, metode overjanja, protokoli.

Preko enotne prijave smo tako omogočili enotno prijavo in povezovanje naše rešitve Connected mHealth z obstoječo rešitvijo klinike Mayo Clinic, prav tako, so lahko pacienti klinike Mayo Clinic, ki so že uporabljali naše rešitve 24alife, sedaj lahko prijavljeni z enakim računom v novo rešitev. Podatki med rešitvami se v kolikor uporabnik to želi, prenesejo iz ene rešitve v drugo, s čimer terapevtom omogočamo, da imajo kompleten in celovit vpogled v pacientovo (uporabnikovo) aktivnost.

4 Strokovnjakova ali pacientova lokacija ne smeta imeti vpliva na prikaz slik in videoposnetkov

V sklopu rešitve Connected mHealth so strokovnjakom in uporabnikom na voljo razni materiali, večinoma v obliki videov in slik, kar nam je predstavljalo tretji večji izziv. Torej, kako zagotoviti hiter prenos slik in videoposnetkov vaj na portal strokovnjaka oziroma na mobilno aplikacijo uporabnika, ki se lahko nahajata širom sveta. Connected mHealth je namreč globalna rešitev, ki pa je locirana na IBM strežniku v ZDA. Geografska razdalja med fizičnim strežnikom, ki se torej nahaja v ZDA in uporabnikom, ki rešitev uporablja npr. v Sloveniji, Angliji, Dubaju ipd., je precejšna, kar pa lahko pomeni tudi do nekaj sekund zamika pri odpiranju vsebine strani.

Za rešitev tega izziva smo se odločili uporabiti rešitev IBM CDN. Kratica CDN izhaja iz angleške zloženke Content Delivery Network. Gre za mrežo proxy strežnikov v številnih podatkovnih centrih po vsem svetu. Osnovna naloga CDN sistema je učinkovito, varno in hitro serviranje vsebin z uporabniku najbližjih strežnikov. To pomeni, da CDN uporabniku vsebino prikaže s strežnika, ki je njemu najbližji. S tem se uporabniku vsebina prikaže hitreje, kar pozitivno vpliva na uporabniško izkušnjo in posledično tudi na večjo uporabo rešitve in zadovoljstvo uporabnikov. Z implementacijo IBM CDN smo tako uporabnikom naše rešitve Connected mHealth, ki so locirani zunaj ZDA zagotovili nemoteno uporabo in serviranje večjih podatkov s strežnikov iz najbližje lokacije.

IBM CDN pa poleg pospeševanja dostave vsebin ponujajo še številne druge prednosti. Vsebine, ki so uporabnikom prikazane prek IBM CDN porabijo manj kot polovico pasovne širine (ang. bandwidth) kot sicer, prav tako pa se nekje v podobnem obsegu zmanjšajo tudi zahtevki za prikaz. Strežnik, na katerem se nahajajo "originalne" vsebine, je torej precej manj obremenjen in se hitreje nalaga, kar omogoča tudi večji promet. Dodatna velika prednost IBM CDN je tudi varnost vsebine, IBM namreč zagotavlja napredne varnostne sisteme, ki preprečujejo možnost prestrezanja in zlorabe podatkov, kar je v današnjih časih zelo dobrodošlo.

Literatura

[1] https://www.keycloak.org/, Open Source Identity and Access Management, obiskano 9.6.2022

[2] https://eurohealthnet.eu/sl/publication/mhealth-provides-opportunities-but-risks-widening-inequalities/, mZdravje ponuja priložnosti, vendar tvega povečanje neenakosti, obiskano 9.6.2022

[3] https://ibmi.mf.uni-lj.si/rehabilitacija/vsebina/Rehabilitacija_2013_S1_p104-111.pdf, TELEREHABILITACIJA V CELOSTNI REHABILITACIJI PACIENTOV, obiskano 29.6.2022

[4] https://www.vortex.si/kaj-je-cdn, Kaj je CDN in kako z njegovo uporabo pohitrimo odzivnost spletne strani?, obiskano 29.6.2022

[5] https://www.optiweb.com/sl/blog/pohitritev-globalne-spletne-strani-s-pomocjo-cdn-storitev/, Pohitritev globalne spletne strani s pomočjo CDN storitev, obiskano 9.6.2022

[6] https://www.cakalnedobe.si/nasvet/telezdravje-telemedicina-kaj-je-kako-deluje/, Telezdravje in telemedicina: Kaj to sploh je in kako deluje?, obiskano 4.7.2022

[7] https://www.ibm.com/docs/sl/planning-analytics/2.0.0?topic=logs-audit-log, Revizijski dnevnik, obiskano 4.7.2022

[8] https://sl.wikipedia.org/wiki/Revizijska_sled, Revizijska sled, obiskano 4.7.2022