Platforma i aplikacija za praćenje pandemije

Abstrakt

Jedan od najvećih problema u borbi sa pandemijom je utvrđivanje liste osoba sa kojima je zaražena osoba bila u kontaktu. Brzim utvrđivanjem liste kontakata i njihovim testiranjem, drastično se povećava efikasnost sprečavanja širenja zaraze.

Najefikasniji način za praćenje kontakata u okruženju je korišćenje modernih 'bluetooth' tehnologija ugrađenih u mobilne telefonske aparate. Za potrebe aplikacije koristi se BLE (Bluetooth Low Energy) interfejs. Potpuna anonimnost zabeleženih kontakata u okruženju se postiže metodom izmenjivih tokena čije trajanje je vremenski ograničeno.

Platforma i aplikacije za praćenje i suzbijanje pandemije moraju tehnološki da zadovolje sve uslove koje zahteva zakon o zaštiti privatnosti podataka, to jest da garantuje anonimnost, bezbednost i privatnost korisnika.

RedDot.zone platforma i aplikacija je moderno, sofisticirano softversko rešenje koje ispunjava sve kriterijume zaštite privatnosti podataka a istovremeno efikasno beleži sve kontakte u okruženju korisnika i omogućava mu da u slučaju zaraženosti sve te kontakte obavesti o mogućnosti zaraze.

Ceo sistem se sastoji od četiri bitne celine: blokčejn platforme, Android i iOS mobilne aplikacije, admin panela i pozadinskog (backend) sistema organizovanog u vidu mikroservisa.

Zaštita podataka i privatnost korisnika

RedDot.zone platforma i aplikacija u potpunosti ispunjavaju sve zahteve Zakona o privatnosti zaštite podataka Republike Srbije, kao i evropske regulative za zaštitu privatnosti podataka GDPR.

Korisnički nalog je potpuno anoniman. Za kreiranje naloga nije potrebno dati ni jedan lični podatak kao što su ime i prezime, adresa, broj telefona, email adresa i slično. Prilikom registracije naloga, korisnik generiše javni i tajni ključ koji se čuva na njegovom uređaju i nikad ga ne napušta, i kojim kriptuje sve svoje podatke, uključujući i listu zabeleženih kontakata u okruženju.

Potpuna anonimnost zabeleženih kontakata u okruženju se postiže metodom izmenjivih tokena. Kada se dve ili više osoba nalaze sa svojim uređajima u blizini od (X) metara, svaki od korisničkih uređaja beleži spisak kodova (tokena) korisničkog ID-a koji se menjaju na svakih 15 minuta i kriptuje ga na svom uređaju privatnim ključem. Korisnik na svom uređaju nije u mogućnosti da vidi tu listu kontakata.

U slučaju zaraženosti, korisnik ima mogućnost, da potpuno anonimno i dobrovoljno, dekriptuje listu zabeleženih kontakata u poslednjih 'X' dana i tako omogući sistemu da pošalje notifikaciju korisnicima sa te liste o mogućoj zaraženosti i preporukom za testiranje.

Kako funkcioniše reddot.zone praćenje kontakata u okruženju?

U momentu kada korisnik instalira aplikaciju, generiše se jedinstven korisnički ID (standardni UUID koji je jedinstven za aplikaciju i biće isti sve do reinstalacije), kao i par ključeva (javni i tajni); korisnički ID uz javni ključ se šalje reddot.zone serveru i korisnik se registruje. Token za push notifikacije se potom šalje na server i čuva u bazi. To su jedina tri podatka koji se čuvaju na serveru (UUID, javni ključ i token za push notifikacije). Na osnovu ovih informacija nemoguće je utvrditi identitet korisnika.

Reddot.zone aplikacija beleži susrete sa drugim korisnicima tako što izmenjuje poruke preko Bluetooth servisa. U cilju zaštite privatnosti korisnika, poruke koje se izmenjuju ne sadrže lako čitljive informacije koje bi mogle odati identitet. Takođe ne sadrže neizmenljiv (ili statičan) sadržaj koji bi se mogao iskoristiti za praćenje određenog korisnika.

Kako se kreiraju ove poruke (ili u daljem tekstu, tokeni)?

Tokene kreira server strana, isključivo na zahtev korisnika, pri čemu svaki token čini korisnikov ID, vreme od kada token traje, vreme do kada token traje, a sve ovo je enkriptovano AES-256-CBC algoritmom. Na ovo se dodaju dva dodatna podatka koji povećavaju nivo zaštite: IV (inicijalni vektor) i 8 bajtova SHA256 hash funkcije. Binarno predstavljeno, token izgleda ovako:

Korisnikov id (16 bajtova)	Od kada traje (4 bajta)	Do kada traje (4 bajta)	IV (16 bajtova)	SHA256 (prvih 8 bajtova)

←----------Enkriptovano sa AES-256---------->

Tokeni, pošto su binarni podaci, se šalju korisniku enkodirani Base64 algoritmom.

Svaki token ima svoje vreme trajanja (aplikacija ‘nudi’ samo token čija je vaznost unutar trenutnog vremena) koje je u ovom trenutku 15 minuta. S obzirom da token ne sadrži lako čitljiv korisnikov ID, time je sprečeno deanonimisanje korisnika, a sa druge strane, kako tokeni traju relativno kratak vremenski interval, tako je sprečeno da treća strana može da lažira nečiji token (kratko trajanje tokena čini ovo nepraktičnim, jer je interval u kome se token može lažirati prekratak).

Kako aplikacija uzima tokene sa servera?

Neposredno po registraciji, aplikacija traži od servera da joj da određeni broj tokena; trenutno se uzima toliko tokena koliko je dovoljno za 3 dana (tokeni traju 15 min). Jednom dnevno aplikacija proverava da li ima vezu sa serverom i dovlači novi skup tokena. Tokeni se čuvaju u SQLite bazi na uređaju.

Kako aplikacija ‘priča’ sa ostalim uređajima?

U osnovi komunikacije je Bluetooth Low Energy (BLE) protocol. Aplikacija implementira Peripheral i Central role, što će reći da ujedno nudi BLE servis (Peripheral rola), ali istovremeno i aktivno skenira okolinu (Central rola) tražeći druge uređaje. U momentu kada aplikacija nađe drugi uređaj (praktično drugog korisnika iste aplikacije) uređaji će razmeniti trenutno važeće tokene (u binarnoj formi, dakle Base64 dekodiranoj) te iste upisati u lokalnu bazu, ovaj put enkriptovane AES-256

algoritmom. Enkripcija se radi u cilju sprečavanja treće strane da dođe do tokena ukoliko ostvari pristup korisnikovom uređaju.

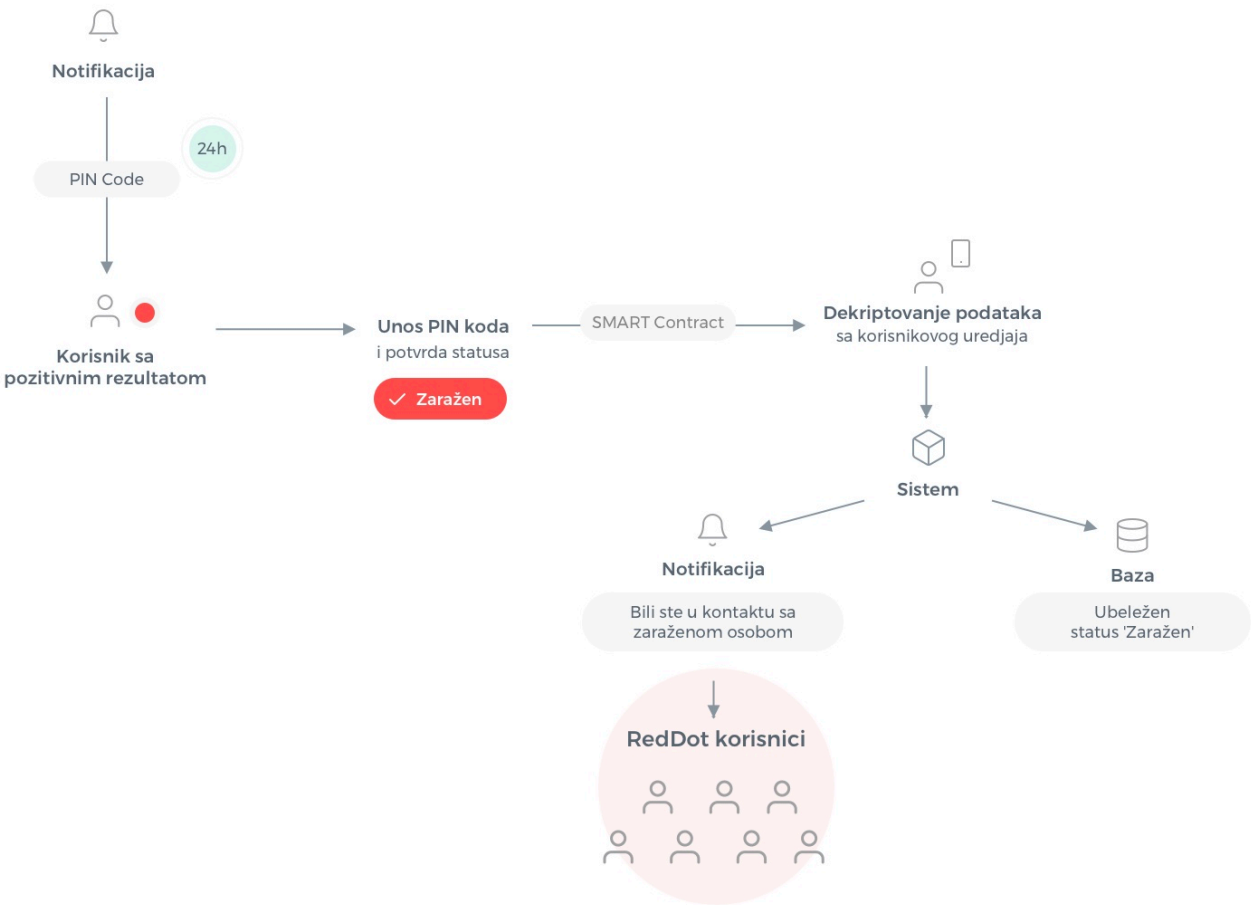
Šta se dešava sa tokenima kada je korisnik zaražen?

U tom trenutku, ukoliko korisnik to eksplicitno dozvoli kroz interfejs u aplikaciji, aplikacija skuplja sve tokene ne starije od 28 dana iz lokalne baze, dekriptuje ih, te šalje na server. Da bi se onemogućila zloupotreba slanje na server je moguće samo uz pomoć koda koji zdravstvena institucija, kroz WWW interfejs generiše na serverskoj strani. S obzirom da su tokeni enkriptovani i na serverskoj strani, server može pročitati korisnički ID iz svakog tokena, te time zaključiti sa kime je korisnik bio u kontaktu tokom perioda od 28 dana. Tim kontaktima se šalje 'push' notifikacija sa obaveštenjem o potencijalnom susretu sa zaraženim. Notifikacije ne sadrže nikakve dodatne informacije o kontaktu, tako da ne postoji mogućnost otkrivanja identiteta zaraženog kontakta.

Dodatni nivo sigurnosti i privatnosti pruža upis u blockchain. Svaka manipulacija tokenima i svaka akcija se upisuju u neizmenljivi registar i može se proveriti. Ovo obezbeđuje da su podaci neizmenjivi i ne mogu se lažirati. S obzirom da je svaki pristup podacima zabeležen, mogućnost zloupotrebe je svedena na minimum. A s obzirom da je minimalan skup podataka koji se prikupljaju o korisniku, nemoguće je pronaći identitet zaraženog korisnika niti osoba sa kojima je ostvaren kontakt.

Procedura notifikacija upozorenja

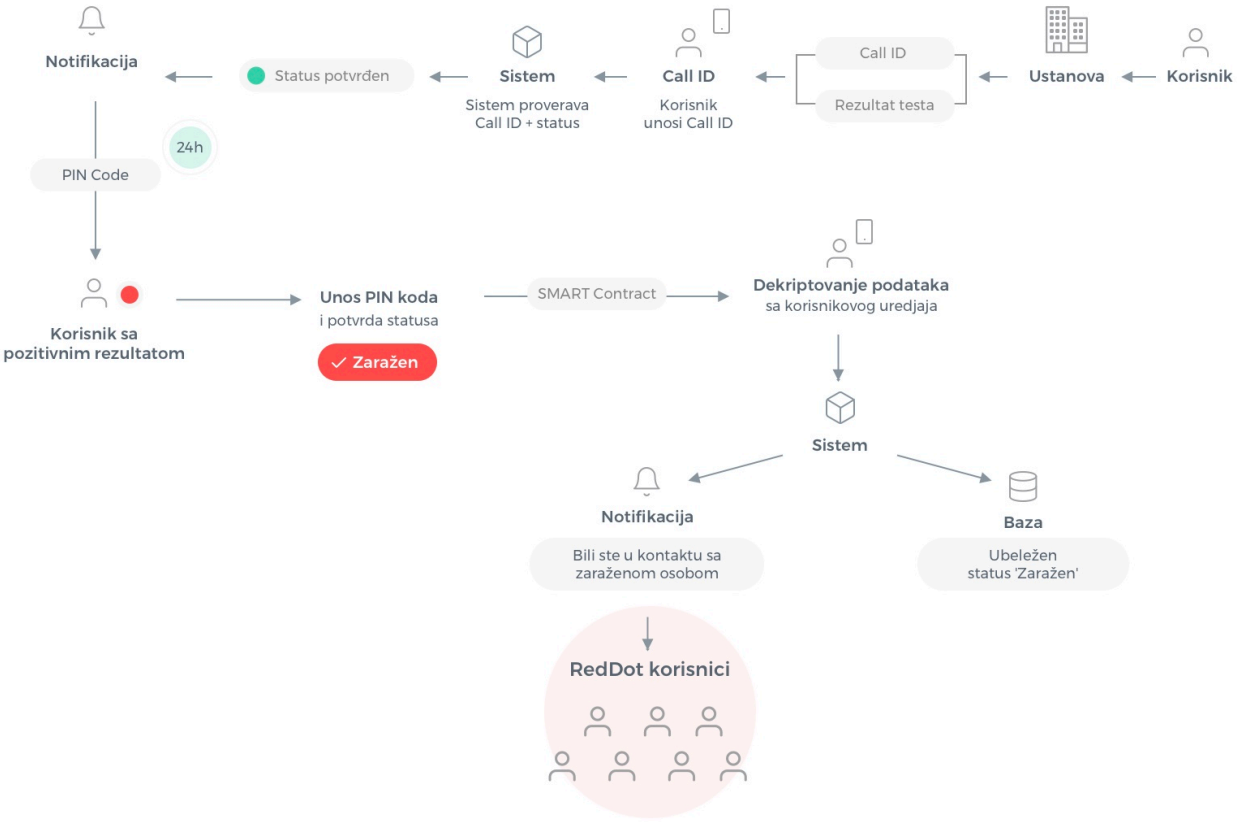
Slučaj 1. Korisnik automatski dobija poruku od sistema da je u nekom periodu bio u kontaktu sa zaraženim korisnikom.



Kada osoba koja je zaražena dobije pozitivan rezultat testa, dobiće od sistema pin kod koji važi 24h u kom roku može dobrovoljno na svom uređaju da potpiše transakciju pritiskom na dugme ‘zaražen :(‘. Time se ‘smart contract’ izvršava i dekriptovani podaci sa korisnikovog uređaja se šalju na sistem i sistem automatski šalje notifikaciju svim korisnicima koji su u bazi registrovani da su poslednjih (X) dana bili u kontaktu sa zaraženim userom, a zaraženi korisnik se u sistemu označava kao zaražen. Sve transakcije moraju da nose time stamp.

Sistem šalje potpuno anonimno generisane kodove korisnicima koji su bili poslednjih (X) dana u kontaktu sa zaraženim korisnikom. Kada user ode da se testira on ne daje svoj user id već kod koji je dobio od sistema.

Slučaj 2. Korisnik aplikacije dobije simptome i ode da se testira a nije dobio kod za testiranje (CallID),



Ustanova je dužna da generiše novi kod iu admin panelu, upiše ga u karton korisnika kao i rezultate testa koji će mu biti uručeni. Ustanova je dužna da to uradi uvek kad vrši testiranje uzorka koji već ne sadrži CallID. Time se obezbeđuje da korisnik koji se testirao a nije prethodno dobio poziv preko aplikacije, kao i budući korisnik aplikacije, obezbedi CallID.

Kada takav korisnik dobije rezultate testa ‘zaražen’ uz rezultate mu je dat i generisani CallID. U aplikaciji na mobilnom telefonu će biti polje ‘Unesi CallID’. Kada korisnik unese podatak, sistem proveri da li taj CallID postoji sa statusom ‘zaražen’, sistem prihvata unos, povezuje (mečuje) tog korisnika sa CallID ‘zaražen’ i automatski šalje notifikaciju korisniku sa pinkodom pomoću kojeg

može da izvrši komandu o zaraženosti i time pošalje dekriptovane liste korisnika sa kojima je bio u kontaktu.

Ograničenja

Zbog tehničkih ograničenja koje ima operativni sistem iOS, aplikacija mora da radi sve vreme u foreground-u, kako bi preko bluetooth uredjaja mogla da detektuje korisnike oko sebe. Čak i ako je samo jedan token primljen od strane iOS aplikacije, smatraće se da je korisnik bio u kontaktu sa zaraženom osobom, iz razloga što ukoliko aplikacija ode u background tada se stopiraju svi servisi i sve dok se aplikacija ponovo ne upali isti korisnik neće moći da dobije drugi token.

Arhitektura platforme

- Blokčejn platforma - blokčejn i smart kontrakt organizovana platforma koja omogućava registrovanje pristupa podacima u tzv. javni registar, čime se sprečava neovlašćen pristup i zloupotreba podataka. Napravljena je na bazi proverenih i testiranih alatki (Bitshares blokčejn pisan u C++ programskom jeziku) 'Elasticsearch' baze podataka, standardni objeknti data store, sofisticiranog API-ja (Application Program Interface) za priključivanje korisničkih aplikacija i najmodernije tehnike enkripcije na strani korisnika.
- Korisnička mobilna aplikacije za Android / iOS platforme - moderna mobilna aplikacija pisana u izvornim 'native' Android (Java) i iOS (Swift) programskim jezicima, sa ugrađenim modulima za 'Bluetooth proximity' senzore, enkripciju na strani uređaja, 'push' notifikaciju
- Administrativni web panel - upravljački interfejs za upravljanje sistemom na strani vlasnika licence. Najmoderniji web panel pisan u HTML, CSS, JavaScript jezicima kome je moguće pristupiti iz desktop i mobilnih alata za pregled (browser-a).
- Čitav pozadinski (backend) sistem je organizovan u vidu mikroservisa. Svaki servis radi na Linux platformi, spakovan je kao Docker kontejner, i po potrebi spreman za rad na Kubernetes platformi. Kao takav, sistem je prenosiv i moguće ga je izvršavati kako na privatnom serveru (ili grupi servera) tako i na javnom ili privatnom cloud-u. Takođe, sistem je skalabilan, tako da je moguće da izdrži opterećenje više miliona korisnika, što se postiže jednostavnim pokretanjem onoliko dodatnih instanci servisa koliko je potrebno i iskorišćavanjem load balancer uređaja.