CARNET

Signal

NCERT-PUBDOC-2018-4-359

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT–a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.

1 Uvod

Privatnost komunikacije osnovno je pravo svakog pojedinca. Sve učestalijim korištenjem tehnologije za komunikaciju javlja se i više načina povrede njene privatnosti. Ako se primjerice koristi servis za razmjenu poruka koji te poruke čuva na svojim poslužiteljima u izvornom, nešifriranom obliku, postoji opasnost da će pružatelj usluga nezakonito čitati te poruke ili da će napadač uspješno napasti poslužitelj i doći do sadržaja poruka.

Ti problemi mogu se riješiti šifriranjem poruka korištenjem ključeva koji su dostupni samo na uređajima korisnika. Na primjer, ako Đuro i Martin razmjenjuju poruke preko svojih mobilnih uređaja, Đuro poruku šifrira tako da samo Martin ima ključ koji ju može dešifrirati. Na taj način, poruku ne može pročitati čak ni vlasnik poslužitelja koji nudi servis razmjene poruka. Takav sustav zaštite komunikacije naziva se šifriranje s kraja na kraj (eng. *end-to-end encryption* ili E2EE).

Iako sustavi koji osiguravaju komunikaciju šifriranjem s kraja na kraj postoje već duže vrijeme, oni su do nedavno uglavnom zahtijevali osnovno razumijevanje kriptografije i složene korake prilikom postavljanja. Zbog toga je veći dio populacije i dalje koristio manje sigurne, ali intuitivnije sustave. Aplikacija „Signal“ nastala je upravo s idejom da bude jednostavna i time lako dostupna za korištenje najširem krugu korisnika, posebice onima koji nisu upoznati s tehničkom pozadinom kriptografije.

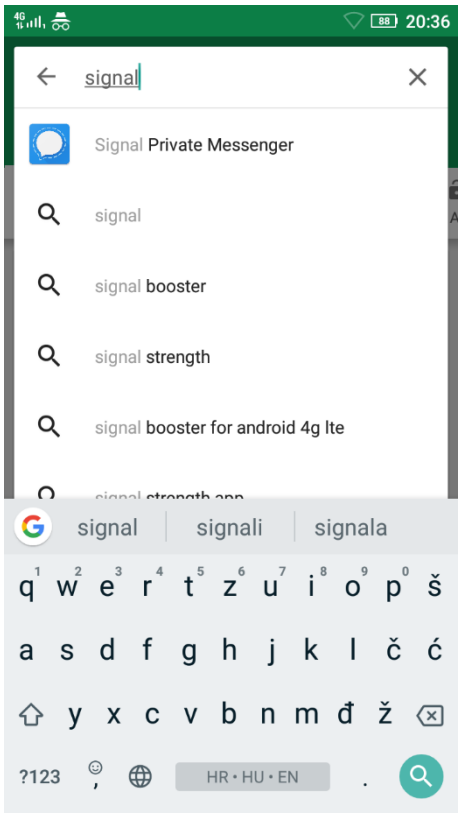
Signal je slobodna aplikacija otvorenog koda (eng. *free and open source – FOSS*) koja omogućava brzu i jednostavnu sigurnu komunikaciju korištenjem šifriranja s kraja na kraj. Zbog toga je brzo stekla veliku popularnost te njeno korištenje preporučuju brojni kriptografski stručnjaci. Istoimeni protokol Signal (kojega koristi aplikacija Signal) napravljen je tako da se može lako implementirati u drugim aplikacijama za razmjenu poruka te ga zato danas koriste popularne aplikacije kao što su WhatsApp i Facebook Messenger. Aplikacija Signal dostupna je na dva najpopularnija operacijska sustava za mobilne telefone – Android i iOS te je dostupna i na popularnim operacijskim sustavima za osobna računala: Windows, Linux i macOS.

U ovom dokumentu bit će opisan postupak instalacije aplikacije Signal te njeno osnovno korištenje.

2 Instalacija aplikacije Signal

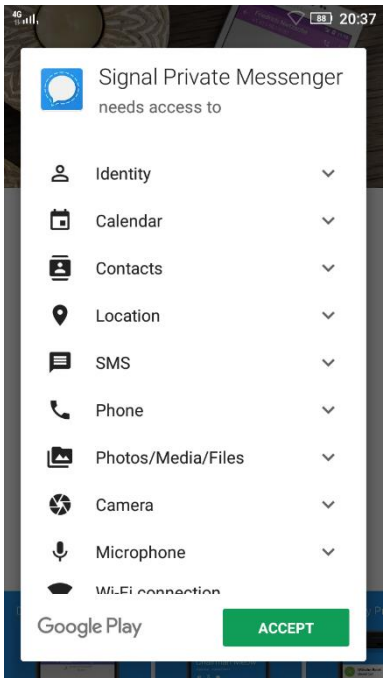
U ovom poglavlju bit će prikazana instalacija aplikacije Signal na operacijski sustav za mobilne uređaje Android. Inačica operacijskog sustava Android na kojoj će se instalirati Signal je 5.1.1. Princip instalacije vrlo je sličan i na ostalim inačicama sustava Android, no može se razlikovati u dodjeljivanju dozvola aplikaciji Signal.

Prvo je potrebno otvoriti aplikaciju ***Google Play*** tj. ***Trgovina Play*** ako je sustav na hrvatskom jeziku. U polje za pretraživanje aplikacija potrebno je unijeti *Signal* te odabrati ***Signal Private Messenger.***

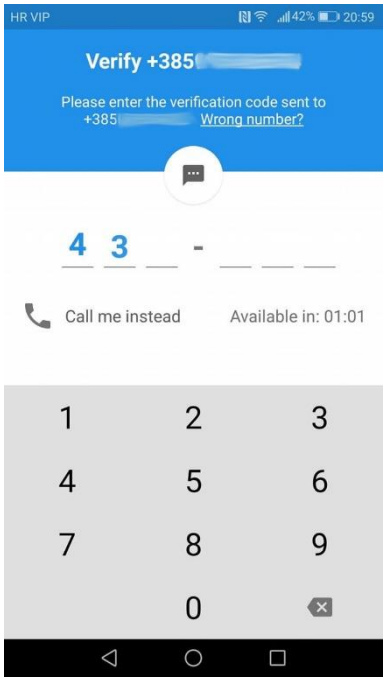


Kako bi Signal bio preuzet s Google Play trgovine, potrebno je dohvatiti tridesetak megabajta. Nakon pritiska na gumb ***Install*** započinje proces instalacije.

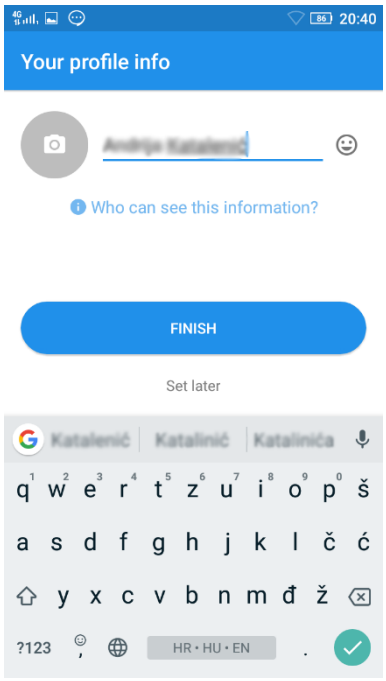
Ovisno o inačici operacijskog sustava Android, u sljedećem koraku može se prikazati prozor za dodjeljivanje dozvola aplikaciji Signal. U inačici Androida u ovom primjeru prikazan je takav prozor, što je vidljivo na donjoj slici. Na ovoj poveznici moguće je pročitati objašnjenja kako Signal koristi svaku od traženih dozvola. Kako je aplikacija Signal otvorenog koda, moguće je pregledom izvornog koda precizno provjeriti kako ona točno koristi dozvole. Najoprezniji korisnici mogu i ručno generirati (eng. *build*) aplikaciju iz izvornog koda te na taj način biti sigurni da izvorni kod koji pregledavaju zaista odgovara aplikaciji koju koriste. Nakon odobravanja dozvola aplikaciji Signal pritiskom na ***Accept*** započinje instalacija na mobilni uređaj.



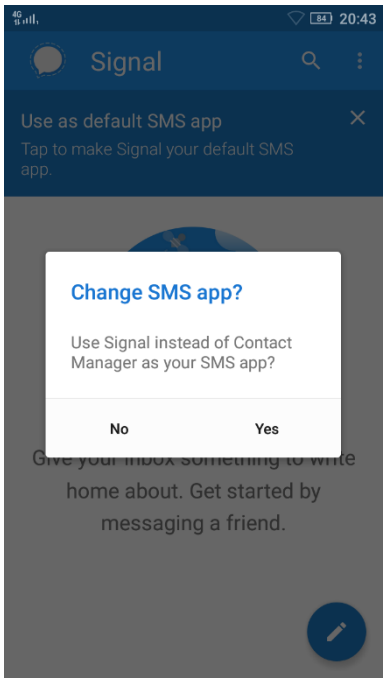
Nakon instalacije, potrebno je pokrenuti Signal. Pri prvom pokretanju prikazuje se korak za registraciju i potvrđivanje broja mobilnog telefona. Nakon unosa broja te pritiska na gumb ***Register*** počinje njegova potvrda. Ako Signal ima dozvole za čitanje SMS poruka kod za potvrđivanje broja poslan SMS porukom će se automatski pročitati. U suprotnom potrebno je *ručno* upisati kod poslan u SMS poruci.



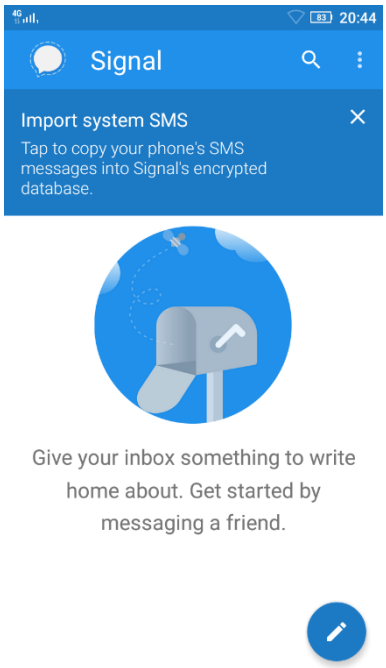
U sljedećem koraku moguće je unijeti ime korisnika tj. njegovog profila u aplikaciji Signal. Nakon unosa imena te klikom na ***Finish*** može se započeti s korištenjem aplikacije Signal.



Signal se također može koristiti i za upravljanje SMS porukama. Ako se ta opcija želi odabrati potrebno je pritisnuti gumb ***Yes***.



Sad se otvara početni pogled aplikacije Signal u kojem je moguće uvesti SMS poruke iz sustava mobitela i u kojem je moguće pregledati razgovore aplikacije Signal, što će biti objašnjeno u sljedećem poglavlju.

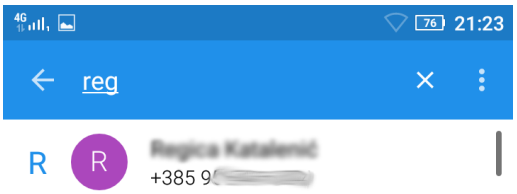


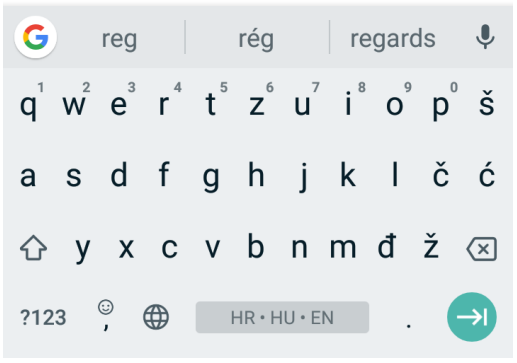
3 Korištenje aplikacije Signal

Iako će korištenje aplikacije Signal ovdje biti ilustrirano na Android platformi, postupci su slični i na ostalim platformama na kojima je Signal dostupan.

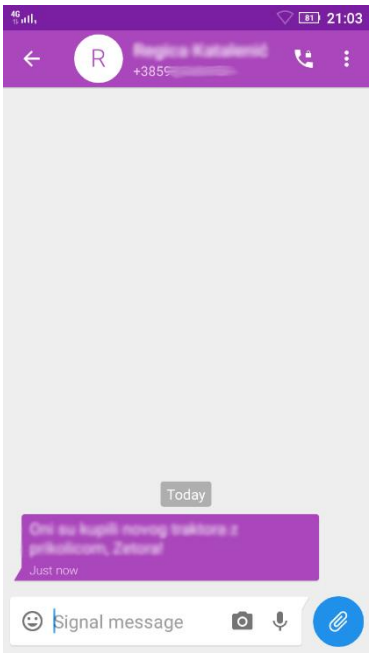
3.1 Slanje poruka

Kako bi mogli slati šifrirane poruke pomoću aplikacije Signal, na početnom ekranu aplikacije potrebno je odabrati razgovor ili pritisnuti na ikonu u donjem desnom uglu kako bi vidjeli dostupne kontakte. Kao što je prikazano na donjoj slici, moguće je vidjeti koji kontakti u imeniku korisnika koriste Signal i filtrirati ispis po imenu.

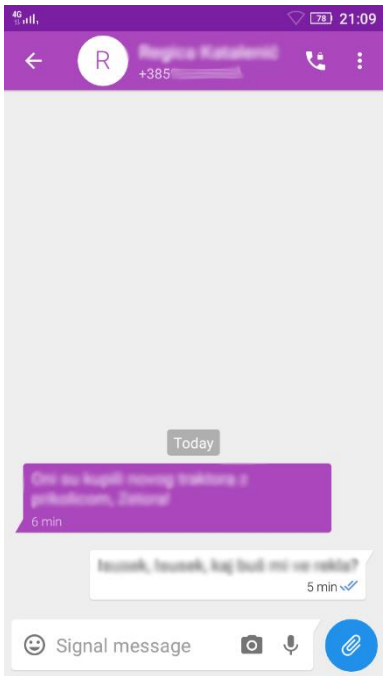




Nakon odabira kontakta otvara se prozor u kojem se mogu upisivati poruke. U donjem primjeru prikazana je dolazna poruka:

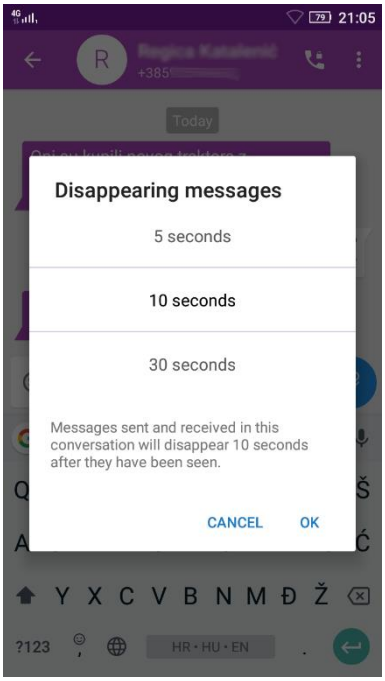


Upisivanjem poruke u okvir za upis teksta i pritiskom na plavu ikonu za slanje poruke šifrirana poruka šalje se drugom korisniku:



3.2 Nestajuće poruke

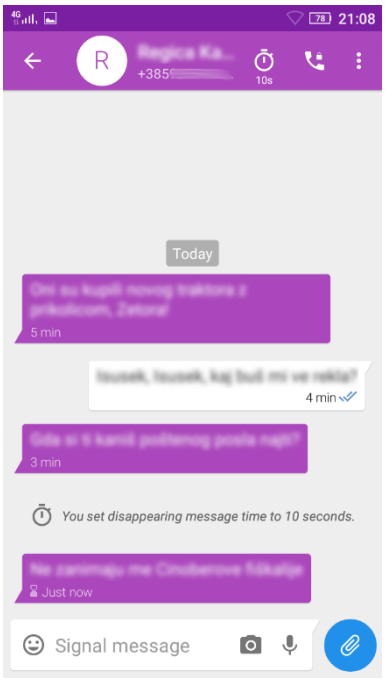
Signal nudi i mogućnost poruka koje nestaju nakon određenog perioda vremena. Kako bi se omogućile nestajuće poruke (eng. *disappearing messages*) potrebno je odabrati ikonu za glavni izbornik te ***Dissapearing messages***. Nakon izbora vremenskog perioda nakon kojega poruke nestaju, pritiskom na ***OK*** ta postavka se aktivira u razgovoru. Drugom korisniku će se pojaviti poruka u kojoj je navedeno kako su nestajuće poruke postavljene.



Postavljeno vrijeme nestajanje poruke počinje teći nakon što je poruka pročitana. Uz nestajuću poruku moguće je primijetiti ikonu pješčanog sata, koja označava koliko dugo će poruka trajati prije nego što će biti izbrisana.

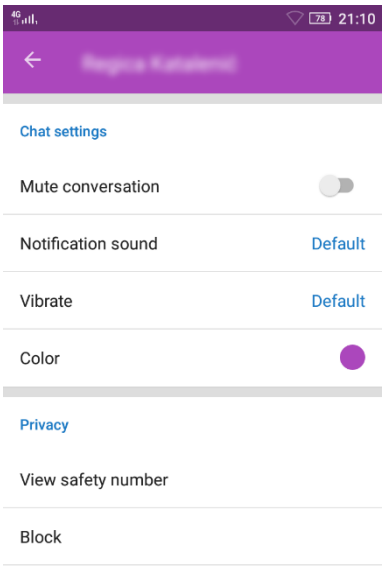
Nestajuće poruke pomažu korisnicima držati povijest poruka urednom. No, nestajućim porukama nije moguće spriječiti primatelja poruke da nekako trajno zabilježi sadržaj poruke, jer čak i uz onemogućeno uzimanje slike trenutnog ekrana, moguće je jednostavno napraviti fotografiju ekrana mobilnog telefona, npr. s drugim mobilnim uređajem.

Primjer nestajuće poruke:

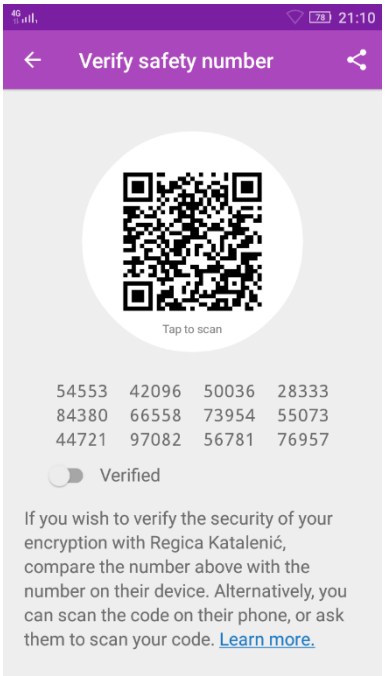


3.3 Provjera sigurnosnog broja

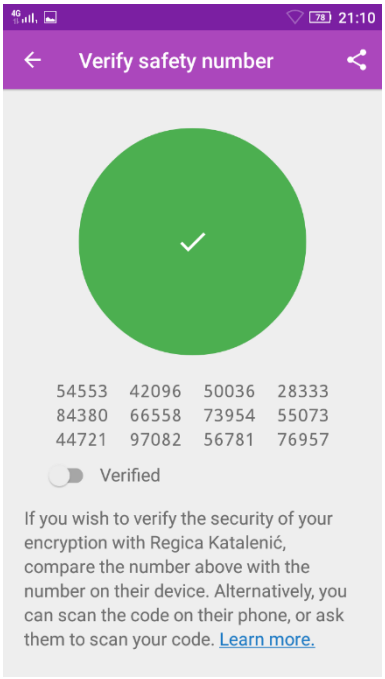
Svaka komunikacija (npr. razgovor između dvoje ljudi) ima jedinstveni sigurnosni broj (eng. *safety number*). Sigurnosni broj omogućava korisnicima aplikacije Signal da potvrde da je komunikacija sigurna od tzv. posredničkih napada (eng. *man-in-the-middle attacks*) – napada u kojima napadač presreće, čita i mijenja sadržaj poruka. Dovoljno je da korisnici jednom potvrde sigurnosni broj njihovog razgovora – nakon toga će njihove buduće Signal poruke i pozivi biti sigurni. Kako bi se taj broj provjerio potrebno je stisnuti ikonu za glavni izbornik (tri vertikalne točke). Nakon toga potrebno je odabrati ***Conversation Settings***.



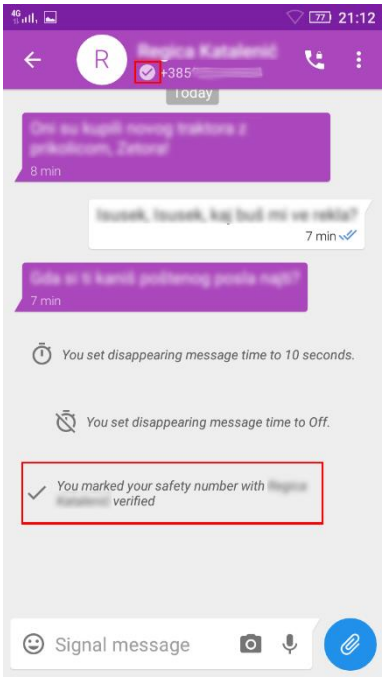
Sada je potrebno pritisnuti ***View safety number*** kako bi se prikazao sigurnosni broj te kako bi se on mogao usporediti s sigurnosnim brojem koji je prikazan drugom korisniku. S tehničke strane, kako je glavni razlog provjeravanja sigurnosnog koda izbjegavanje posredničkih napada, nije poželjno sigurnosne brojeve provjeravati preko Signal poruka. Sigurnosni broj najbolje je provjeriti uživo ili nekim sigurnim kanalom komunikacije, npr. telefonski. Dostupno je i jednostavno skeniranje QR koda kako bi proces provjere broja bio što brži.



Pritiskom na QR kod aktivira se kamera mobilnog telefona te je moguće skenirati QR kod na drugom mobilnom telefonu. Ako se brojevi podudaraju, prikazuje se zeleni krug kao na donjoj slici.

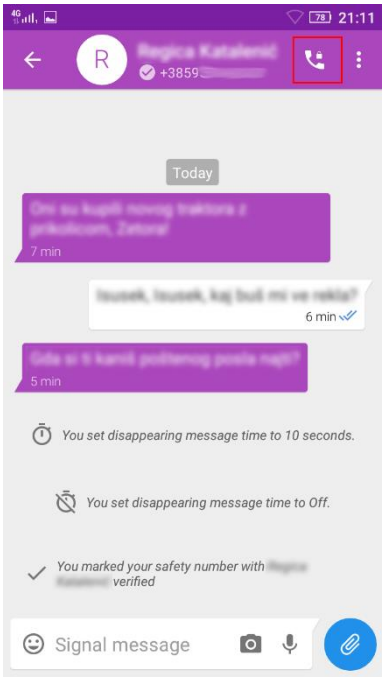


Sada je također moguće klizač *Verified* prebaciti u aktivan položaj, kako bi Signal pamtio koji kontakti su potvrđeni sigurnosnim kodom. Nakon potvrđivanja, uz ime kontakta se sada nalazi ikona s kvačicom, što se može vidjeti u donjoj slici:

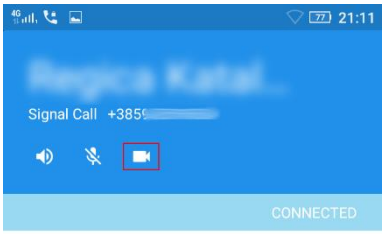


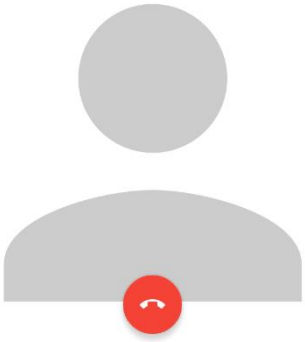
3.4 Ostvarivanje poziva

Kako bi se započeo šifrirani poziv, unutar razgovora s drugim korisnikom potrebno je pritisnuti ikonu s telefonskom slušalicom.



Nakon toga aplikacija korisniku koji se poziva javlja da ima poziv te se čeka da ga on prihvati. Nakon što je drugi korisnik prihvatio poziv, na ekranu se ispisuje *Connected*:

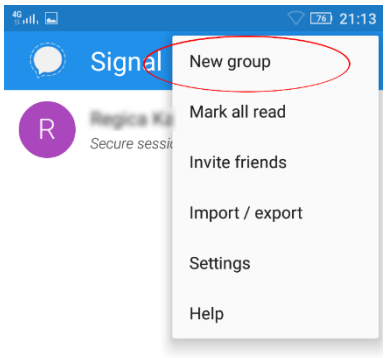




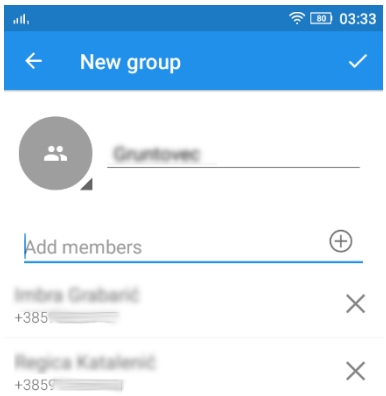
Signal također podržava i video pozive, a kako bi se takav poziv ostvario, unutar običnog poziva potrebno je pritisnuti ikonu za kameru, označenu crvenim pravokutnikom u gornjoj slici.

3.5 Grupni razgovor

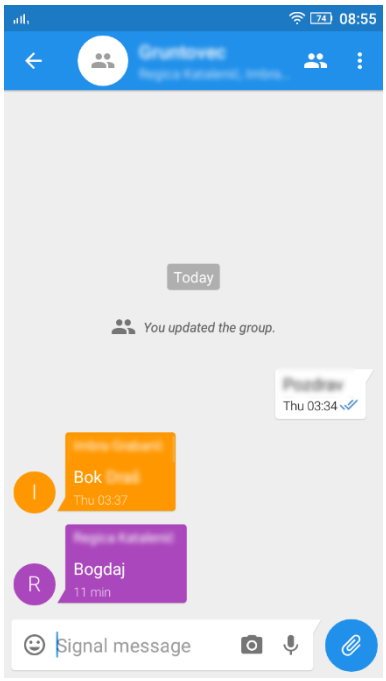
Stvaranje grupnog razgovora moguće je ostvariti otvaranjem glavnog izbornika pritiskom na ikonu s tri točke te odabirom na ***New Group***.



Nakon toga je moguće imenovanje grupe i dodavanje drugih korisnika u grupu. Ako neki kontakt u imeniku nema Signal, već se aplikacija Signal koristi i za SMS i MMS poruke, Signal će upozoriti da se stvara MMS grupa.

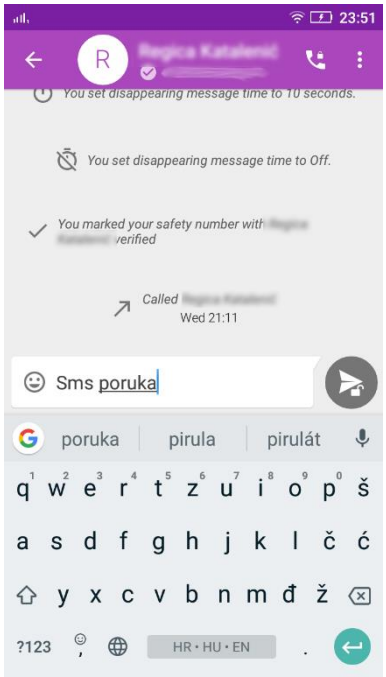


Sada svaki korisnik može slati poruke u grupu:



3.6 Slanje SMS poruka

Ako je odabran kontakt koji koristi Signal, a želi mu se poslati SMS poruka, potrebno je pritisnuti plavu ikonu za slanje te odabrati ***SMS Message***. Ikona za slanje se tada mijenja u sivu boju te lokot koji je otključan. Razlog tome je nemogućnost aplikacije Signal da šifrira SMS poruke, tako da se one ne šalju šifrirane Signalovim protokolom.



4 Zaključak

Signal je aplikacija za razmjenu poruka koja koristi napredne kriptografske algoritme za osiguravanje komunikacije. Kao što je moguće vidjeti kroz opis osnovnog korištenja aplikacije Signal, ona svojom jednostavnošću približava korištenje sigurne, šifrirane komunikacije širokom krugu korisnika. Sigurna komunikacija ostvarena je bez zahtijevanja da korisnik posjeduje napredna tehnička znanja ili dublje razumijevanje kriptografije.

Pri korištenju aplikacije Signal, bitno je imati na umu kako je za potpunu zaštitu potrebno provjeriti podudarnost sigurnosnih brojeva u određenom razgovoru. Provjeravanjem podudarnosti sigurnosnih brojeva potvrđuje se da je zbilja ostvaren siguran komunikacijski kanal između krajnjih korisnika aplikacije.

Kroz više godina postojanja aplikacije i istoimenog protokola, Signal se pokazao kao pouzdano i sigurno rješenje te ga preporučuju brojni sigurnosni stručnjaci – između ostaloga i poznati kriptografski stručnjak Bruce Schneier. Aplikacija i protokol Signal se i dalje aktivno razvijaju te se protokol implementira u sve većem broju alata i zasigurno će u skoroj budućnosti biti još važniji alat za osiguravanje privatnosti korisnika.