DEEP MESSENGER PROTOKOL 1 ALPHA4

UVOD

Ovaj dokument opisuje prvu verziju protokola koja se koristi za izmjenu i kontrolu poruka među instancama Deep Messenger aplikacije i Deep Messenger Mailbox servisa.

OSNOVNA STRUKTURA OKVIRA PORUKE

Sve poruke definirane u ovom protokolu započinju sa dva polja duljine 1B, prvo polje sadrži verziju protokola, odnosno u ovom slučaju broj 1, ukoliko klijent zaprimi poruku koja sadrži neispravnu verziju dužan je prekinuti vezu. Drugo polje sadrži tip poruke, ukoliko klijent zaprimi neispravan tip poruke dužan je prekinuti vezu. Nakon navedena dva polja slijede dodatna polja i podaci koji ovise o tipu poruke.

VER	MESSAGE TYPE	DATA
1	1	DEPENDS ON THE MESSAGE TYPE

Za sve tipove poruka definirane ispod, navedena su samo polja koja se nalaze u DATA dijelu dijagrama iznad, te se podrazumijeva da ispred njih dolaze polja VER i MESSAGE TYPE.

Svi tipovi poruka koji sadrže ID transakcije moraju ga dostaviti kao prvo polje radi lakšeg odbacivanja neispravnih poruka. MESSAGE TYPE polje svih poruka koje sadrže ID transakcije i čija se izmjena vrši nakon uspostave transakcije mora imati bit najveće težine postavljen na 1 radi praktičnije implementacije.

TIP PORUKE: TRANSACTION REQUEST (0x01) – REQ

Prije nego što dva klijenta mogu početi komunicirati preko socketa potrebno je započeti transakciju. Klijent koji je započeo vezu šalje zahtjev za uspostavu, a drugi klijent tada odgovara sa porukom TRANSACTION RESPONSE koja sadrži UUID ove transakcije. Taj ID transakcije vrijedi samo za taj connection i čim se veza prekine oba klijenta će zaboraviti da je postojao. Na ovaj način čak i ako netko uspije uhvatiti jedan od potpisanih paketa ne mogu se predstaviti kao netko drugi jer transaction ID neće odgovarati.

S obzirom da transakcija još nije započela nema smisla da klijent išta potpisuje ili se predstavlja, stoga je ovo jedini tip poruke koji nema tijelo.

TIP PORUKE: TRANSACTION RESPONSE (0x02) – RES

Ovim tipom poruke odgovara klijent koji je zaprimio TRANSACTION REQUEST i inicijalizirao transakciju za ovaj socket. Tijelo poruke sadrži samo 16 bajta koji predstavljaju UUID ove transakcije. Ovom porukom je transakcija započela i sve poruke koje se nadalje izmjenjuju sadrže dani transaction ID, ako poruka ne sadrži odgovarajući transaction ID smatra se da je poruka komprimitirana i veza se prekida.

TRANSACTION ID	16

TIP PORUKE: FRIEND REQUEST (0x81) – REQ

Kako bi dva klijenta mogla izmjenjivati poruke moraju jedan drugog smatrati prijateljima. Prilikom uspostave prijateljstva klijenti izmjenjuju podatke koji im omogućuju da izmjenjuju poruke direktno (peer-to-peer) ili putem mailbox servera. Svaki friend request sadrži slijedeće podatke.

TRANSACTION ID	16
SENDER ONION	62
SIGNING PUB KEY	32
ENCRYPTION PUB KEY	270
MAILBOX ONION	62
MAILBOX ID	16
NICKNAME LEN	1
NICKNAME	4-255
SIGNATURE	64

TRANSACTION ID generirani UUID za ovu transakciju (poruku).

SENDER ONION .onion adresa pošiljatelja.

SIGNING PUB KEY javni ključ ED25519 generiran samo za dani kontakt, odnosno klijenta kojeg tražimo da nam postane prijatelj. Primatelj pohranjuje ključ i koristi ga za buduće predstavljanje i potpisivanje poruka koje šalje.

ENCRYPTION PUB KEY javni je ključ tipa RSA 2048 bita. Također ga pohranjuje primatelj, koristi ga kako bi enkriptirao sadržaj poruke koji šalje. Odnosno kako bi enkriptirao simetrični ključ koji se koristio za enkriptiranje poruke. Ključ je enkodiran u DER obliku, i kao takav javni ključ je dug 270 bajta (testirano).

MAILBOX ONION .onion adresa mailbox-a koji pošiljatelj koristi. U slučajevima kada pošiljatelj nije online, ali primatelj mu želi poslati poruku može kontaktirati njegov mailbox server na ovoj adresi. Ukoliko klijent ne koristi mailbox server ovo polje mora biti ispunjeno nulama.

MAILBOX ID kako jedan mailbox server može koristiti više klijenata, ovo je broj pretinca pošiljatelja na koji je potrebno slati poruke. Ukoliko klijent ne koristi mailbox server ovo polje mora biti ispunjeno nulama.

NICKNAME LEN duljina nadimka (korisničkog imena) u bajtovima. Može sadržavati vrijednost između 4 i 255, jer je 4 najmanja dopuštena duljina nadimka. Ukoliko je duljina nadimka manja od 4, odbaciti zahtjev.

NICKNAME niz bajtova koji predstavljaju ASCII znakove korisničkog imena, duljina niza definirana je u NICKNAME LEN polju i ne može biti manja od 4.

SIGNATURE potpis gore navedenih podataka koristeći ED25519 ključ .onion adrese pošiljatelja. Ovim potpisom potvrđujemo da je pošiljatelj stvarno onaj tko se predstavlja. Ukoliko je potpis neispravan, zahtjev nije validan i odbacuje se.

Kada klijent zaprimi FRIEND REQUEST, odgovara sa ACK ONION porukom. Nakon što je korisnik potvrdio da želi biti prijatelj danom klijentu, odgovara na način da šalje svoj FRIEND REQUEST tom klijentu. Kada klijent odgovori sa ACK ONION prijateljstvo je uspješno uspostavljeno.

TIP PORUKE: ACK ONION (0x82) – RES

Jednostavna poruka koja potvrđuje da je dani zahtjev uspješno zaprimljen ili odrađen. Sadrži TRANSACTION ID trenutne transakcije kako bi bio nevažeći van te transakcije.

TRANSACTION ID	16
SIGNATURE	64

TRANSACTION ID generiran za trenutni TCP connection (stream).

SIGNATURE potpis podataka ED25519 ključem onion domene.

Ovaj tip odgovora koristi se kod zaprimanja zahtjeva za prijateljstvo ili zaprimanja poruke na mailbox servisu.

TIP PORUKE: ACK SIGNATURE (0x83) – RES

Poput i ACK ONION odgovora ovaj odgovor se također koristi kao potvrda za odrađeni zadatak.

TRANSACTION ID	16
SIGNATURE	64

TRANSACTION ID generiran za trenutni TCP connection (stream).

SIGNATURE potpis ED25519 ključem koji smo izmijenili prilikom zahtjeva za prijateljstvo (FRIEND REQUEST).

Ovaj odgovor se koristi pri komunikaciji među klijentima, npr. kada klijent pošalje poruku drugom klijentu ovaj mu odgovara sa ACK SIGNATURE kako bi potvrdio primitak poruke.

TIP PORUKE: MESSAGE CONTAINER (0x84) – REQ/RES

Ovo je najčešće korišteni tip poruke, ovaj tip poruke je spremnik koji koristimo kada šaljemo tekstualne poruke i još neke kontrolne poruke kao što je npr. obavijest o promjeni mailbox-a ili korisničkog imena. Sve poruke koje kao klijent šaljemo na mailbox drugog klijenta su ovog formata kako bi sve izgledale identično.

TRANSACTION ID	16
RECEIVER MAILBOX ID	16
SENDER SIGNING KEY	32
MESSAGE ID	16
DATA LEN	4
DATA	VAR
DATA KEY	512
DATA IV	16
SIGNATURE	64

RECEIVER MAILBOX ID nasumičnih 16 bajta koji predstavljaju pretinac na mailbox serveru u koji šaljemo poruku. Ukoliko šaljemo poruku klijentu ovo polje mora biti ispunjeno nulama.

SENDER SIGNING KEY javni ključ tipa ED25519 koji smo dostavili prilikom zahtjeva za prijateljstvo.

TRANSACTION ID generirani UUID koji identificira transakciju.

MESSAGE ID nasumično generirani jedinstveni ID poruke.

DATA LEN broj bajta koji slijedi u DATA dijelu poruke, mora biti najmanje 1 u suprotnom se poruka odbacuje.

DATA sami podaci koji se prenose, enkriptirani simetričnim ključem pohranjenim u DATA KEY polju. Nakon dekripcije prvi bajt predstavlja tip poruke pohranjene u spremniku. Ovisno o tipu poruke različita je i struktura same poruke.

MESSAGE CTYPE	1
DATA	VAR

Dopuštene vrijednosti MESSAGE CTYPE polja (Message Content Type) su:

- TEXT (0x01) – Obična tekstualna poruka, ostatak poruke se interpretira kao poruka koju je klijent poslao.
- NICK (0x02) – Izmjena nickname-a koji klijent koristi i postavljanje novog koji je naveden u bajtovima koji slijede, ukoliko je dani nickname previše dug višak će biti odbačen.
- MBOX (0x03) – Postavljanje novog mailboxa za klijenta koji šalje poruku. Prvih 16 bajta je mailbox id na novom mailbox-u i zatim slijedi 62 bajta koji su onion adresa novog mailboxa.
- RECV (0x04) – Dojava da je dana poruka uspješno dostavljena, nakon tipa polja slijedi 16 bajta koji označavaju UUID poruke.

DATA KEY simetrični ključ tipa AES 256 CBC korišten za enkripciju podataka, enkriptiran RSA javnim ključem dostavljenim u polju ENCRYPTION PUB KEY prilikom zahtjeva za prijateljstvo.

DATA IV je nepredvidljivi nasumično generirani broj koji se koristi kod AES CBC simetrične enkripcije.

SIGNATURE potpis ED25519 privatnim ključem koji odgovara ključu dostavljenom u polju SENDER SIGNING KEY.

Ukoliko bilo koja od validacija poput validacije potpisa ili duljine određenih dijelova poruke ne bude uspješna, mailbox ili sam klijent (ovisno kome je poruka upućena) odmah će zatvoriti vezu, bez ikakvog odgovora. Ukoliko su sve validacije uspješno prošle Klijent će odgovoriti odgovorom ACK SIGNATURE, a Mailbox sa ACK ONION.

TIP PORUKE: MAILBOX REGISTER (0x85) – REQ

Ovaj tip poruke koristi se prilikom registracije na novi mailbox. Nakon što korisnik aplikacije unese .onion adresu svog novog mailboxa i pristupni ključ (ukoliko mailbox nije javan), ovakva poruka se šalje kako bi se registrirao na mailbox.

TRANSACTION ID	16
ACCESS KEY LEN	4
ACCESS KEY	VAR
SIGNING PUB KEY	32

ACCESS KEY LEN duljina ACCESS KEY polja u bajtovima. Ukoliko se klijent registrira na javni mailbox server ovo polje je postavljeno na 0.

ACCESS KEY pristupni ključ generiran na mailbox serveru. Radi se o nizu random znakova kojim klijent dokazuje da ima dopuštenje registrirati se na mailbox serveru.

TRANSACTION ID generirani UUID koji označavaju transakciju.

SIGNING PUB KEY javni ključ tipa ED25519, koristi se za autentikaciju klijenta u danjoj komunikaciji sa serverom. Klijent odgovarajućim privatnim ključem potpisuje sve poruke koje šalje mailbox serveru.

U slučaju kada je ACCESS KEY LEN postavljen na 0, ACCESS KEY nije definiran.

Ukoliko je ACCESS KEY ispravan ili se radi o javnom mailbox serveru, server će odgovoriti sa MAILBOX GRANTED odgovorom. U suprotnom će samo zatvoriti vezu.

TIP PORUKE: MAILBOX GRANTED (0x86) – RES

Nakon što je klijent zatražio mailbox pretinac na danom mailbox serveru, ukoliko je priložio ispravan pristupni ključ, server će odgovoriti ovim tipom poruke.

TRANSACTION ID	16
MAILBOX ID	16
SIGNATURE	64

MAILBOX ID broj pretinca na mailbox serveru koji je dodijeljen klijentu koji je zatražio registraciju.

TRANSACTION ID generirani UUID kopiran iz MAILBOX REGISTER poruke.

SIGNATURE potpis podataka ED25519 ključem onion domene mailbox-a.

Nakon što se je klijent uspješno registrirao na mailbox server, može proslijediti svoj novi MAILBOX ID i MAILBOX ADDRESS svim svojim kontaktima.

TIP PORUKE: MAILBOX FETCH (0x87) – REQ

Pribavi sve poruke sa mailbox servera.

TRANSACTION ID	16
MAILBOX ID	16
SIGNATURE	64

MAILBOX ID jedinstveni broj pretinca klijenta koji traži listu poruka.

TRANSACTION ID generirani UUID transakcije.

SIGNATURE potpis ED25519 privatnim ključem koji odgovara javnom ključu dostavljenom prilikom registracije na mailbox server.

Server odgovara sa tipom poruke MESSAGE LIST.

TIP PORUKE: MAILBOX SET CONTACTS (0x88) – REQ

Postavi kontakte za svoj pretinac na mailbox serveru. Mailbox server će zanemariti sve kontakte koji su bili proje postavljeni i od primitka na dalje će koristiti novu listu kontakata.

TRANSACTION ID	16
MAILBOX ID	16
CONTACTS LEN	2
CONTACTS	VAR
SIGNATURE	64

MAILBOX ID jedinstveni broj pretinca klijenta koji dodaje kontakt.

CONTACT LEN broj kontakata koje želimo postaviti za danog klijenta. Mailbox će u ime klijenta prihvatiti poruke samo od kontakata koji su na listi.

CONTACTS lista blokova po 32 bajta duljine CONTACT LEN koji predstavljaju ED25519 javne ključeve svakog od kontakata na listi.

TRANSACTION ID generirani ID transakcije.

SIGNATURE potpis ED25519 privatnim ključem koji odgovara javnom ključu dostavljenom prilikom registracije na mailbox server.

Ukoliko je operacija uspješna server odgovara sa ACK ONION porukom.

TIP PORUKE: MAILBOX DEL ACCOUNT (0x89) – REQ

Briše registrirani pretinac sa mailbox servera, uključujući i sve podatke unutar pretinca.

TRANSACTION ID	16
MAILBOX ID	16
SIGNATURE	64

MAILBOX ID jedinstveni broj pretinca klijenta koji se odjavljuje sa servera.

TRANSACTION ID generirani ID transakcije.

SIGNATURE potpis ED25519 privatnim ključem koji odgovara javnom ključu dostavljenom prilikom registracije na mailbox server.

Mailbox odgovara sa ACK ONION porukom.

TIP PORUKE: MAILBOX DEL MESSAGES (0x8A) – REQ

Nakon što je klijent uspješno obradio i pohranio poruke koje je pribavio sa mailbox servera, ovim tipom poruke javlja serveru da obriše poruke prema transaction ID-u.

TRANSACTION ID	16
MAILBOX ID	16
IDS LEN	2
MESSAGE IDS	VAR
SIGNATURE	64

MAILBOX ID jedinstveni broj pretinca klijenta.

TRANSACTION ID generirani UUID trenutne transakcije.

IDS LEN broj poruka koje brišemo, ukoliko je postavljen na 0, server ne briše ništa, ali svejedno vraća uspješan odgovor.

MESSAGE IDS lista blokova od 16 bajta, gdje je svaki blok message id poruke koju treba obrisati, duljina liste jednaka je vrijednosti u IDS LEN polju.

SIGNATURE potpis ED25519 privatnim ključem koji odgovara javnom ključu dostavljenom prilikom registracije na mailbox server.

Mailbox odgovara sa ACK ONION porukom.

TIP PORUKE: CLIENT FETCH (0x8B) – REQ

Pošalji upit danom klijentu za listu poruka koje ima za tebe, ukoliko je upit ispravan klijent odgovara sa listom svih poruka za koje nije dobio obavijest da su zaprimljene.

TRANSACTION ID	16
SENDER SIGNING KEY	32
SIGNATURE	64

SENDER SIGNING KEY javni ključ tipa ED25519, generiran za vrijeme zahtjeva za prijateljstvo. To je ključ koji je klijent poslao primatelju kako bi mogao provjeriti poslane poruke.

TRANSACTION ID predstavlja UUID trenutne transakcije.

SIGNATURE potpis, potpisan privatnim ključem koji odgovara ključu u polju SENDER SIGNING KEY.

Kao odgovor na ovu poruku klijent šalje MESSAGE LIST poruku. Ukoliko ne postoji niti jedna ne dostavljena poruka, klijent odgovara sa praznom listom.

TIP PORUKE: MESSAGE LIST (0x8C) – RES

Šalje se kao odgovor na FETCH poruke. Koristi se kako bi dostavili listu MESSAGE CONTAINER poruka.

TRANSACTION ID	16
MESSAGES LEN	32
MESSAGES	VAR
SIGNATURE	64

MESSAGES LEN broj poruka koje se šalju u nizu koji slijedi.

MESSAGES niz MESSAGE CONTAINER poruka. S time da se šalju cijele poruke uključujući VER i MESSAGE TYPE polja. Klijent koji zaprimi poruke, dužan je napraviti validaciju za svaku od poruka i odbaciti sve neispravne poruke, te poslati serveru zahtjev za brisanje.4

SIGNATURE potpis privatnim ključem ED25519, ukoliko ovaj odgovor šalje mailbox server, ovo je potpis ključem onion domene, u suprotnom radi se o ključu čiji je javni dio poslan prilikom zahtjeva za prijateljstvo.