Signal

B	Palvelu ei sovellu kaikkiin käyttötarpeisiin. (Lue lisää)

Ei EU	Palvelu tuotetaan kokonaan tai osittain EU/ETA-alueen ulkopuolella. Asiakas on vastuussa eurooppalaisten tietosuoja- ja tietoturvavaatimusten toteutumisesta. (Lue lisää)

Signal

https://signal.org/

Signal on kommunikaatiosovellus Android- ja iOS-käyttöjärjestelmille. Se käyttää päästä päähän -salausta turvaamaan kaikki toisille Signalin käyttäjille tehdyt ääni- ja videopuhelut ja heille lähetetyt viestit. Sen käyttäjät voivat itsenäisesti todentaa viestien ja puheluiden koskemattomuuden. Chrome-sovellus on myös kehitteillä (ollut käytössä Chromen beta versiossa 7.4.2016 lähtien).

Signalia kehittää Open Whisper Systems. Sen asiakasohjelmien lähdekoodit on julkaistu GPLv3 lisenssin alla. Signal korvasi v. 2015 aiemmat OpenWhisperSystemisin RedPhone ja TextSecure sovellukset yhdistyen yhdeksi sovellukseksi = Signal.

Tehokkaasti kryptattu viestintäsovellus Android- ja iOS-laitteille. Saatavilla myös työpöytäsvellus selaimeen (Google Chrome).

- Signalin käyttäjät voivat soittaa toisilleen puheluita ja lähettää toisilleen pikaviestejä Internet-yhteyden kautta. Sekä puheluissa että viesteissä on salausmahdollisuus.

Käyttöehdot ja tietosuojakäytännöt

- Käyttöehdot vain englanniksi https://signal.org/legal/#terms-of-service
- Tietosuojakäytännöt vain englanniksi https://signal.org/legal/#privacy-policy

Arvio (10.12.2018)

⊕ Päästä päähän salaus mahdollinen
⊕ Yhteentoimivuus useiden muiden pikaviestimen kanssa
⊕ Puhelujen ja viestien salausmahdollisuus
⊕ Asiakasohjelmien lähdekoodit on julkaistu GPLv3 lisenssin alaisuudessa
⊕ Koodi on tarkasteltavissa kokonaisuudessaan ulkopuolisten toimesta
⊕ Ryhmäkeskustelujen mahdollisuus
⊕ Multimedian liittämisen mahdollisuus
⊕ Viesteille voi säätää ajastuksen, jolloin sovellus poistaa viestin lähettäjältä sekä vastaanottajalta
⊕ Toimii Android ja iOS puhelimissa

⊖ Signal vaatii että ensisijainen laite on Android- tai iOS-pohjainen älypuhelin, jolla on nettiyhteys

Kirjautuminen

- Palveluun kirjaudutaan matkapuhelinnumerolla. Palvelu aktivoidaan varmistustekstiviestillä. Palvelua käytetään matkapuhelinsovelluksella, joka voi olla aina taustalla auki.
- Signal vaatii, että ensisijainen laite on Android- tai iOS-pohjainen älypuhelin, jossa on Internet-yhteys

Tukimalli

- Palvelun tukisivusto https://support.signal.org/hc/en-us

Palvelun tarjoaja

- Signal.org (https://signal.org)
- Ohjelman taustalla on vapaaehtoisista muodostuva avoimen lähdekoodin kehittäjätiimi.

Vastaavat palvelut

- WhatsApp, Telegram, Chatsecure, Bleep

Yleiset huomiot:

Palvelussa mobiililaitesovellukset lähettävät toisilleen ns. päästä päähän kryptattuja viestejä (forward secrecy, end-to-end), palvelun perustoiminta ja käyttötarkoitus on hyvin samanlainen kuin paremmin tunnettu WhatsApp. Palvelussa on pyritty monin tavoin varmistamaan, että viestiä ei voi kaapata eikä muokata matkan varrella, eikä siihen voi lisätä ylimääräisiä vastaanottajia.

Ansaintamalli: Signal on voittoa tavoittelematon hanke, jota rahoitetaan joukkorahoituksella ja lahjoituksilla. Palvelun tekninen kuvaus löytyy tukisivustolta http://support.whispersystems.org

Tietoturva ja tietosuoja: Kaikki käytetty ohjelmistokoodi on vapaasti tarkistettavissa GitHubissa. Signal lienee tämäntyyppisistä palveluista ainoa, jonka kaikki ohjelmistokoodi on sellaisenaan tutkittavissa, myös välityspalvelimissa käytetty.

Palvelussa käytetään keskitettyä välityspalvelinta, joka välittää viestit ja tarkistaa käyttäjän osoitekirjasta, keillä viestintäkumppaneilla on käytössään Signal. Välityspalvelinten tarkkaa sijaintia ja kokoonpanoa ei ole kuvattu, mutta niitä kerrotaan ylläpidettävän lahjoitusvaroin ja ne ovat oletettavasti USA:ssa. Palvelimet eivät voi nähdä viestien sisältöä kryptauksesta johtuen, mutta välitystiedot (esim. aikaleima, julkinen salausavain, laitteen push-ID sekä IP-osoite) voivat olla jonkin viranomaisen kaapattavissa.

Mahdolliset viestintäkumppanit selvitetään vertaamalla käyttäjän puhelimessa olevan osoitekirjan puhelinnumerot Signalin asiakastietokantaan. Vertailualgoritmi kuvaillaan yksisuuntaiseksi siten, että käyttäjän osoitekirjan sisältö ei ole selvitettävissä palvelimella.