Sicurezza e Didattica a distanza

A cura di:
MvtinaPwn

Argomenti

- End-To-End Encryption
- Piattaforme dad a confronto
- Piattaforme di messaggistica istantanea a confronto
- Dati raccolti dalle Aziende
- Consigli utili

Domande da porsi durante l’utilizzo di programmi dedicati alla DAD o allo Smart Working(e per qualsiasi altra applicazione)

- Sono realmente sicuri i programmi che utilizziamo tutti i giorni?
- Quali dati vengono da noi esposti involontariamente?
- Chi ha accesso a questi dati?
- Cosa possiamo fare e quali sono i programmi migliori per la nostra privacy?

E2EE (End to End Encryption)

Sistema di comunicazione cifrata nel quale solo le persone che stanno comunicando possono leggere i messaggi.

È l'obiettivo di sicurezza che dovrebbe utilizzare ogni applicazione di collaborazione remota (applicazioni di messaggistica, videoconferenza, scambio di dati…)

È una comunicazione che non permette nemmeno al gestore dell'applicazione di osservare i messaggi scambiati tra gli utenti.

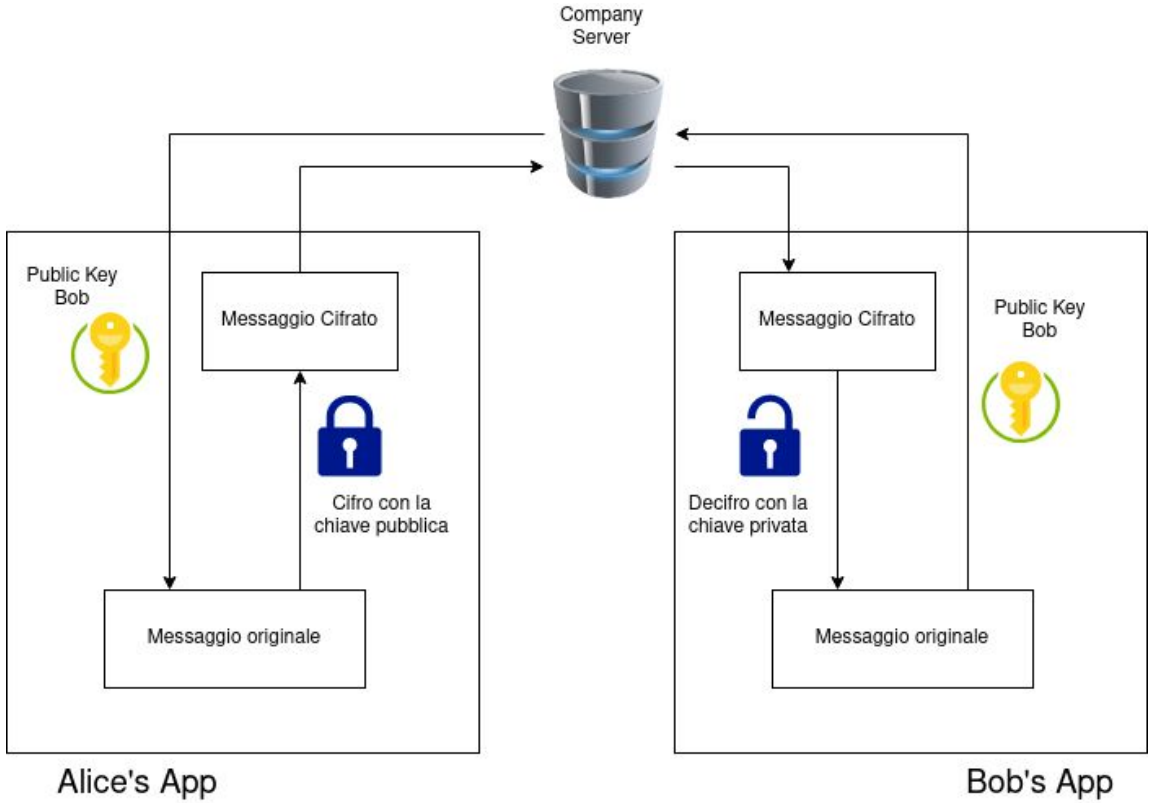
Perchè E2EE è il sistema più sicuro ad oggi?

Perchè cifrando i messaggi prima dell'invio il canale di comunicazione può anche essere insicuro che tanto il messaggio non è leggibile.

Non è necessario l'utilizzo di protocolli di comunicazione sicuri come SSL/TLS.

È l'applicazione stessa che si occupa della cifratura e decifratura della comunicazione.

Schema Crittografia E2EE



Dove “viene” usata la E2EE?

- Applicazioni di Messaggistica: WhatsApp, Telegram, Signal..
- Chiamate e Videoconferenze: Zoom, Discord, Meet, Teams.. (DOVREBBE)
- Scambio di documenti e dati

In queste applicazioni bisogna inoltre considerare se la crittografia End to End in messaggistica o videoconferenza è tra sole due persone oppure tra molti partecipanti

Crittografia E2E nelle Videoconferenze

Google Meet:

È cifrato il traffico tra l'utente e i server di Google.
Google è in grado di vedere i dati in chiaro della stanza.
Utilizza una Secure-by-design infrastructure basata su DTLS-SRTP

Microsoft Teams:

Stessa storia di Meet.
Sono in grado di vedere il traffico in chiaro.
Utilizza TLS-SRTP, unica differenza appunto utilizzo di TLS classico usando pacchetti TCP invece che pacchetti UDP

Zoom:

Da poco ha lanciato una versione che implementa E2EE anche se ancora in fase di testing e con qualche vincolo(es. N° massimo di persone nella stanza)
L'azienda non è in grado di vedere il traffico delle stanze

Discord:

Molto leggero.
Sicurezza minima.
Raccolta di dati degli utenti molto elevata.

Crittografia E2E in Messaggistica

Meglio delle Videoconferenze ma non sempre.

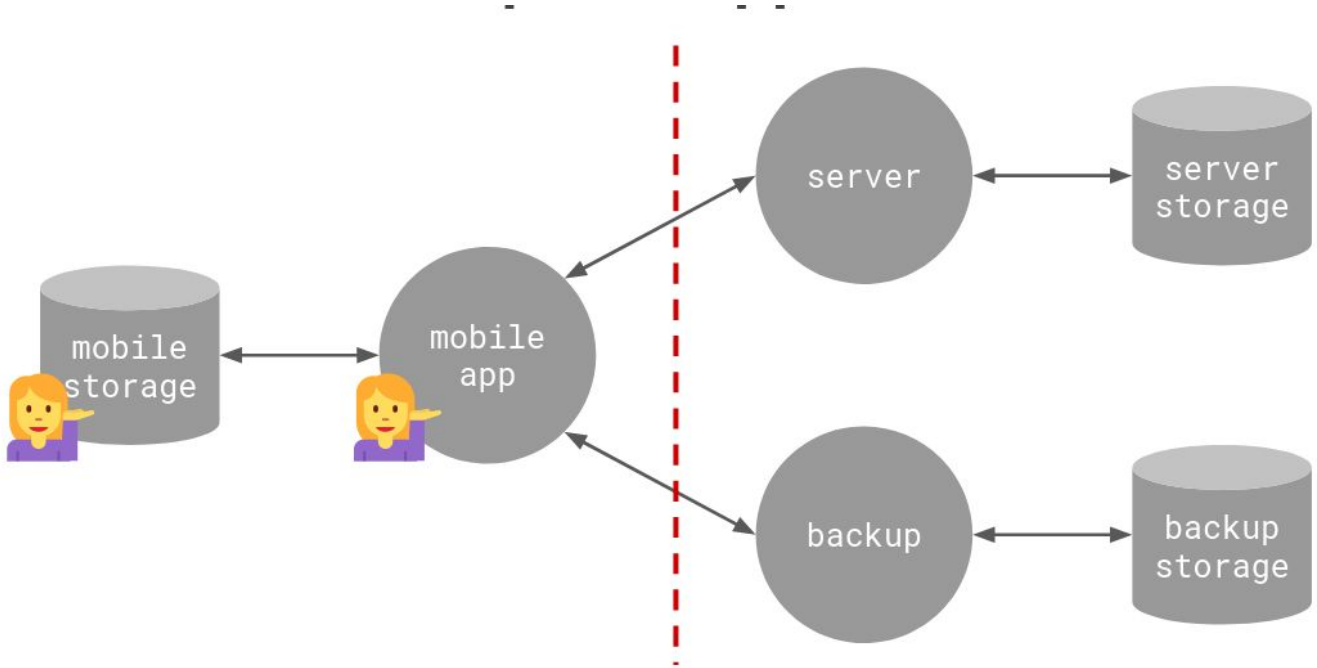
Attenti alle applicazioni di messaggistica che usate!

Crittografia E2E in Messaggistica

Da poco analizzate da Cyber Saiyan in collaborazione con esperti di sicurezza e ex sviluppatori di Signal e WhatsApp le 3 applicazioni più usate in messaggistica:

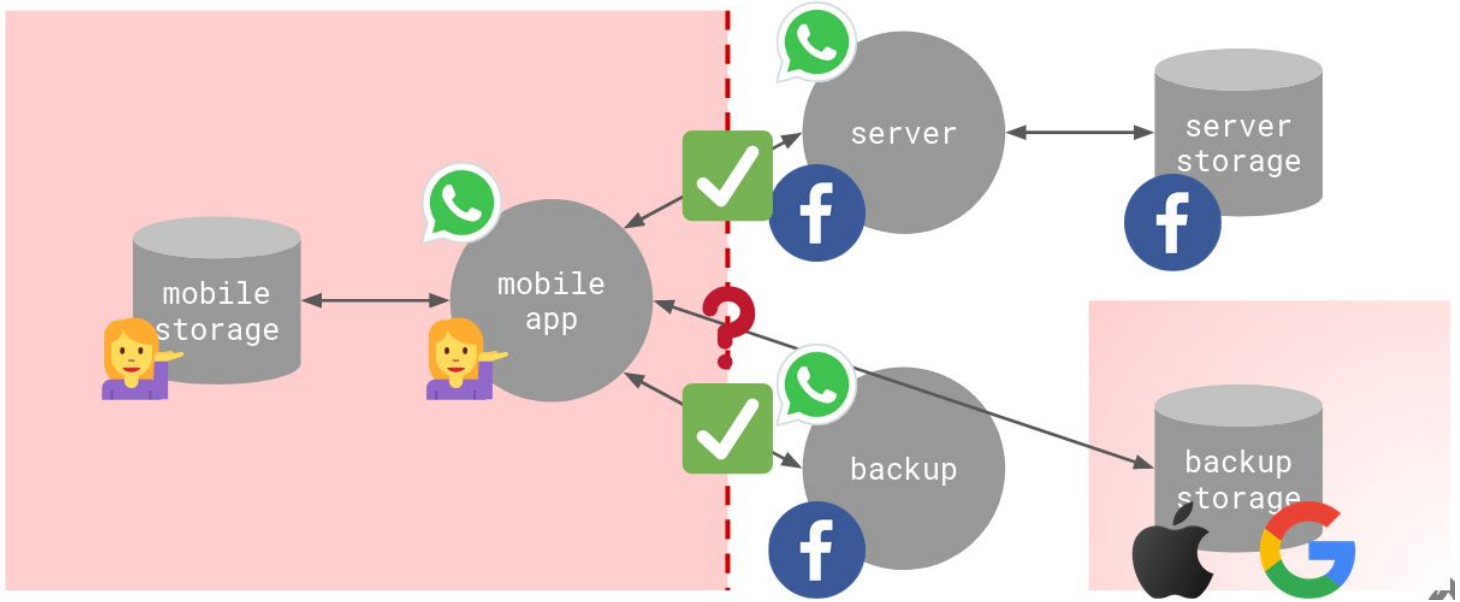
- WhatsApp
- Telegram
- Signal

Tipica Architettura App



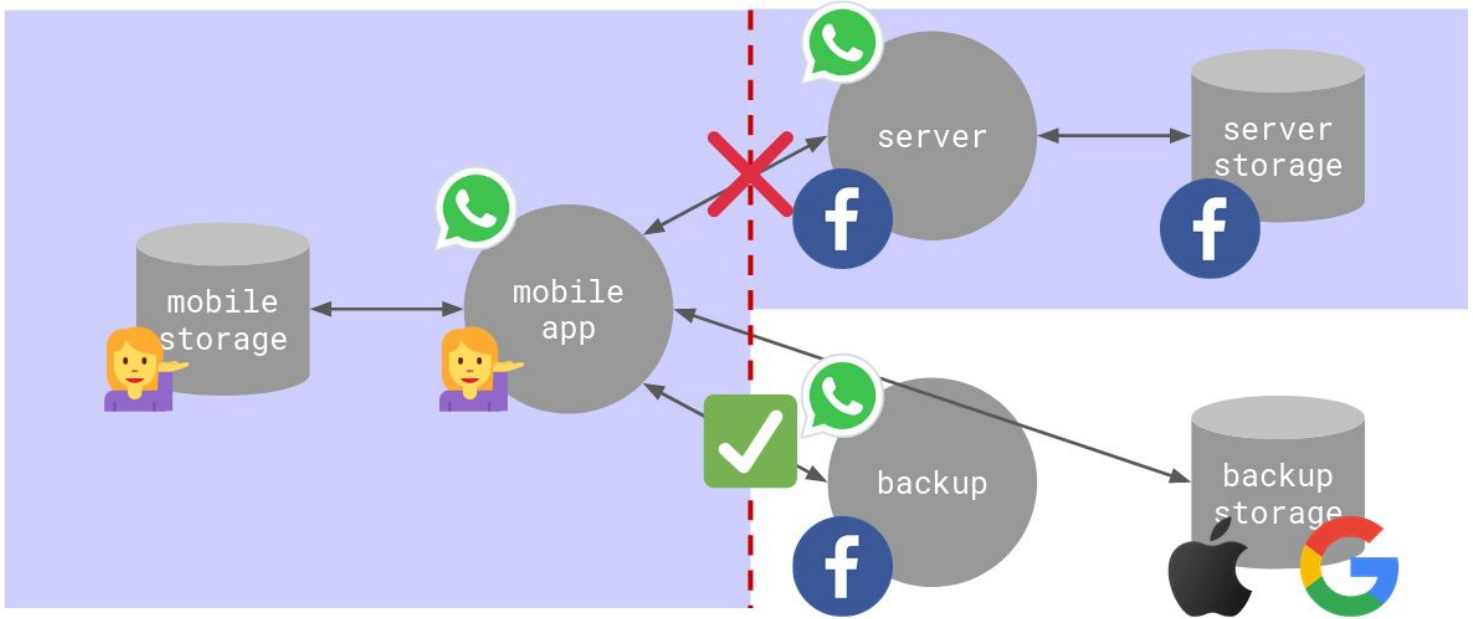
WhatsApp E2EE

Messaggi Visibili solo sull'applicazione, garantita cifratura E2E ma non per i media dei backup su google.
E2EE di Default in tutte le chat



WhatsApp Metadati

Metadati mandati dall'applicazione ai server di Whatsapp (Facebook) che possono visualizzarli.
Vengono invece cifrati durante il backup

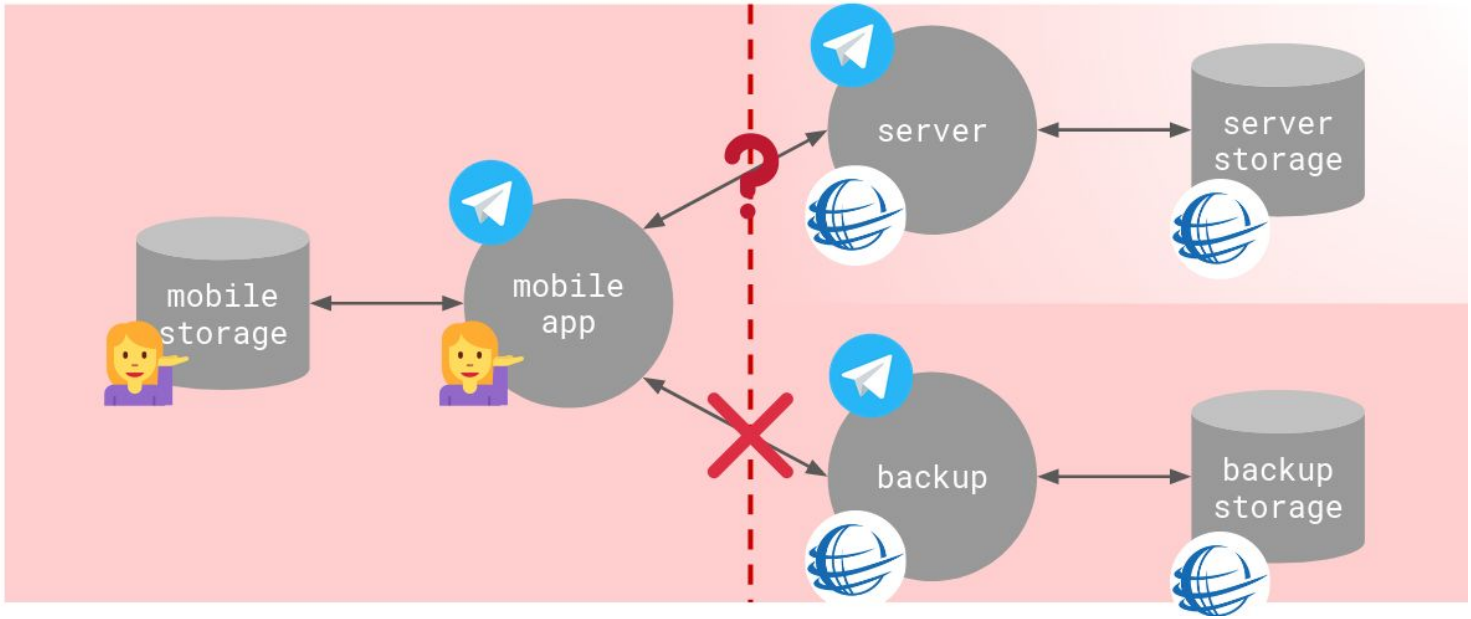


Telegram di Default

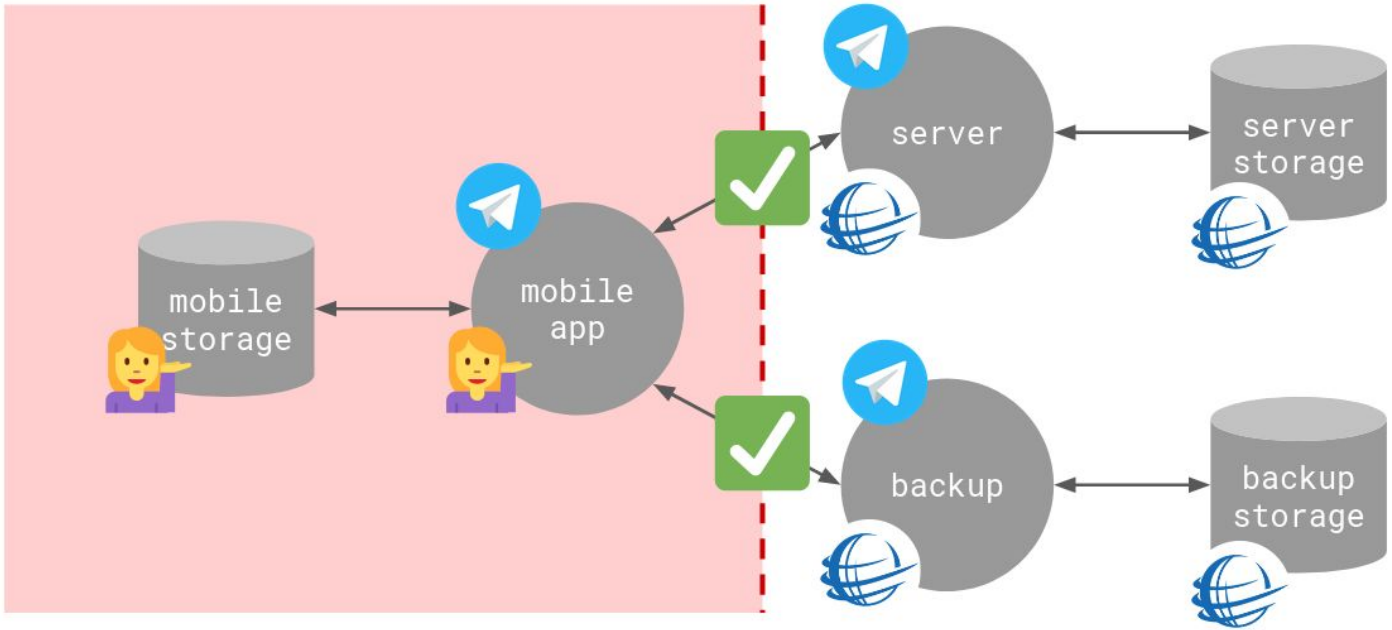
E2EE **NON** di default bisogna usare Chat Segrete.

Tutte le conversazioni sono salvate sui server di telegram in chiaro non cifrate.

Chiamate Audio e video End-To-End



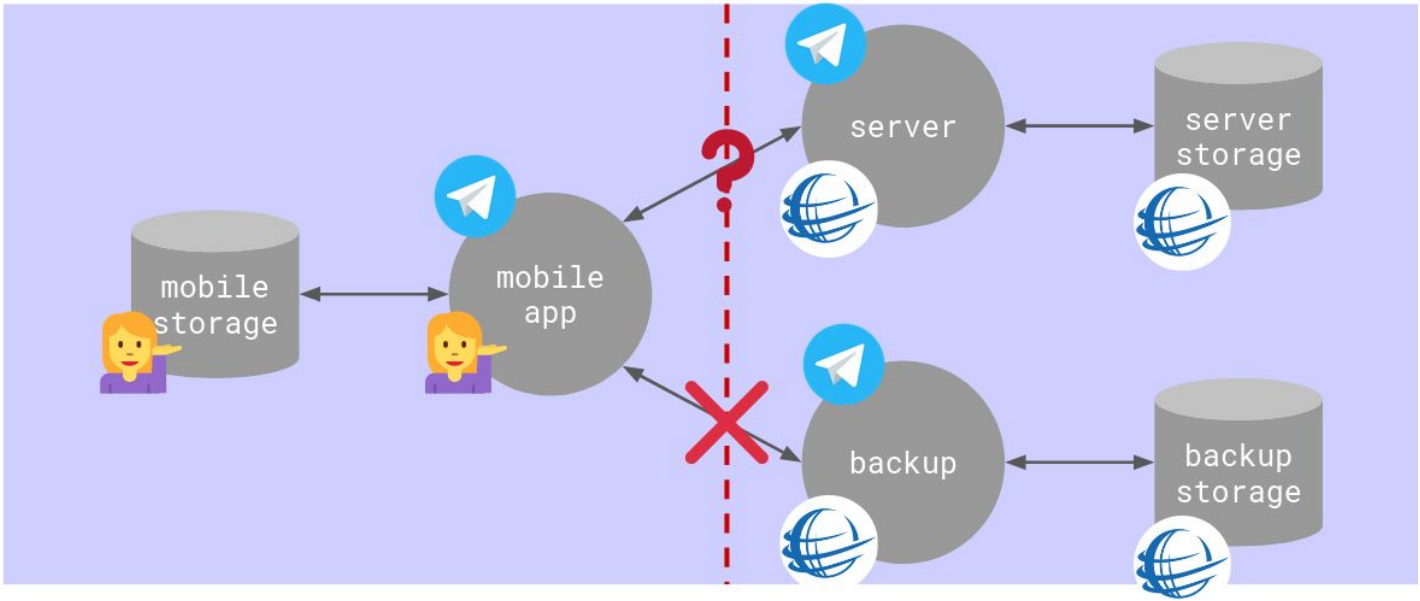
Telegram Chat Segrete



Telegram Metadati

Metadati Salvati sui Server di Telegram Perfettamente visibili da Telegram

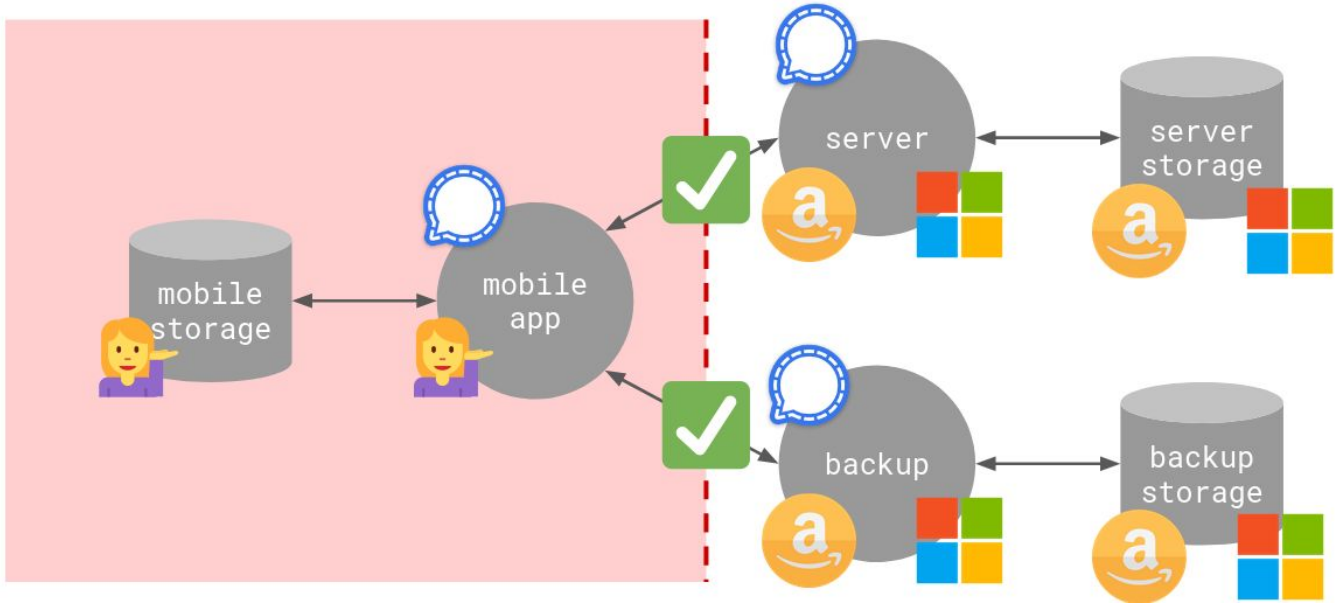
Unica Differenza rispetto a Signal e WhatsApp è che il numero di telefono può essere nascosto



Signal E2EE

Dal punto di vista dei contenuti signal garantisce che siamo gli unici proprietari dei nostri dati

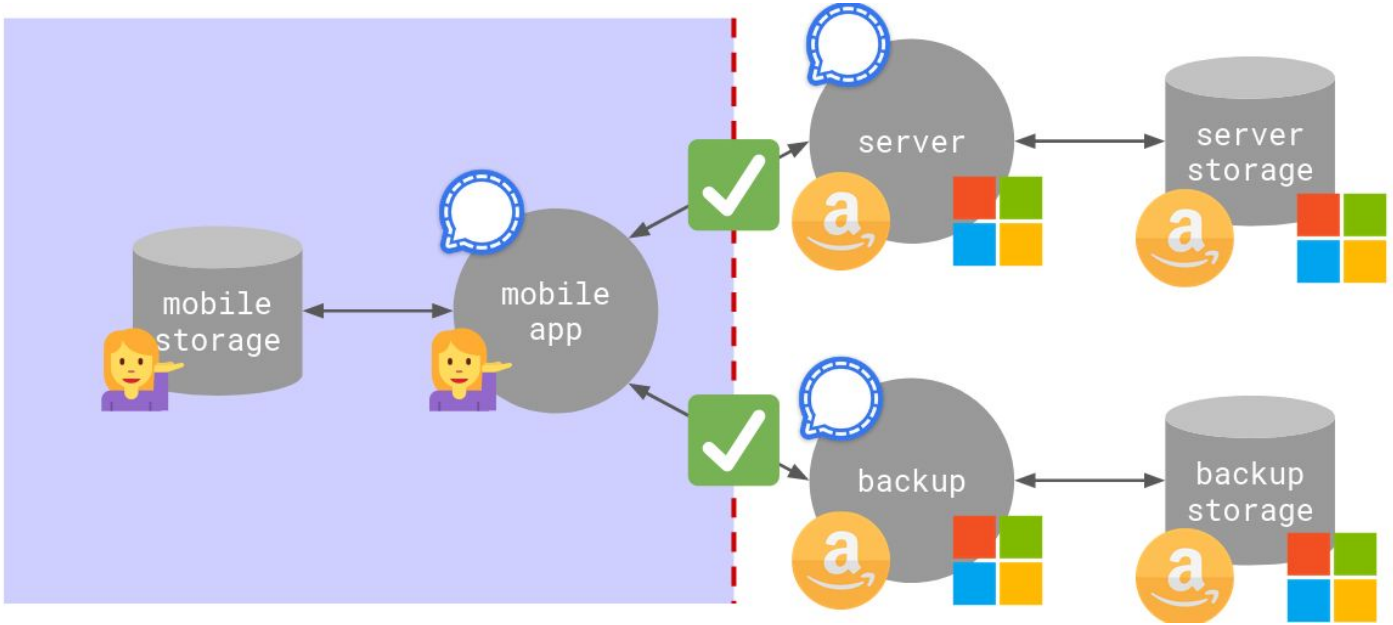
Chiave di backup locale scelta dall'utente con un pin.



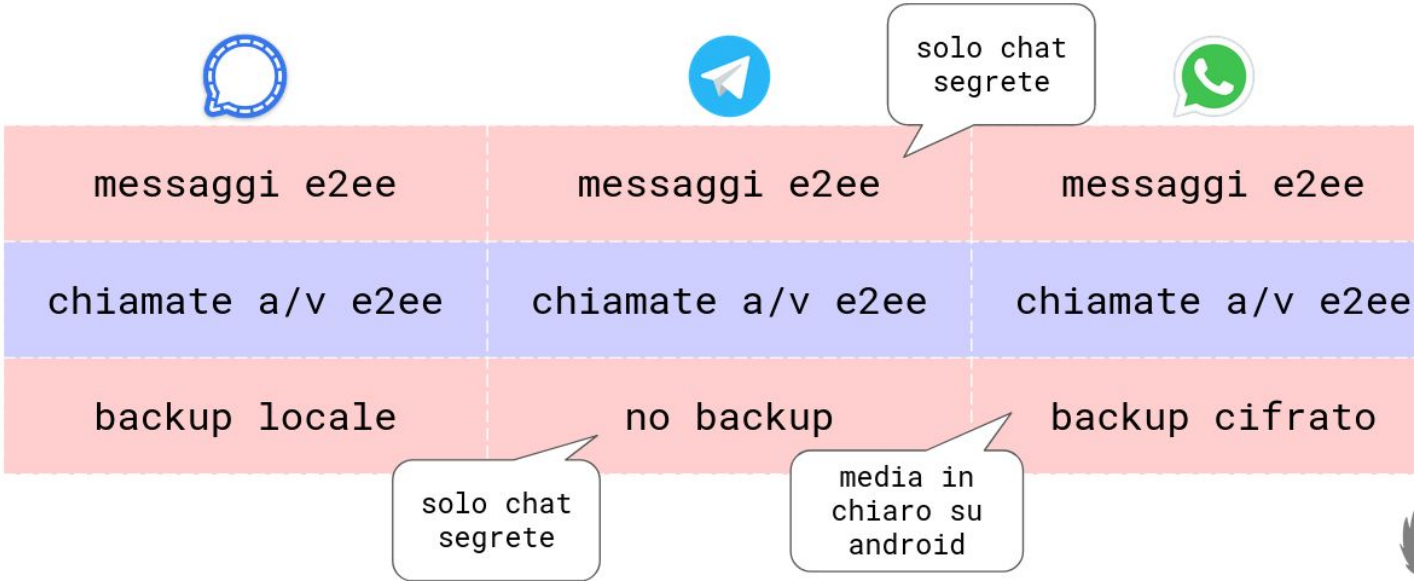
Signal Metadati

Nemmeno la lista dei miei contatti viene inviato a signal.

L’unica che implementa soluzioni tecniche per proteggere i metadati.



Riassunto Protezione Contenuti

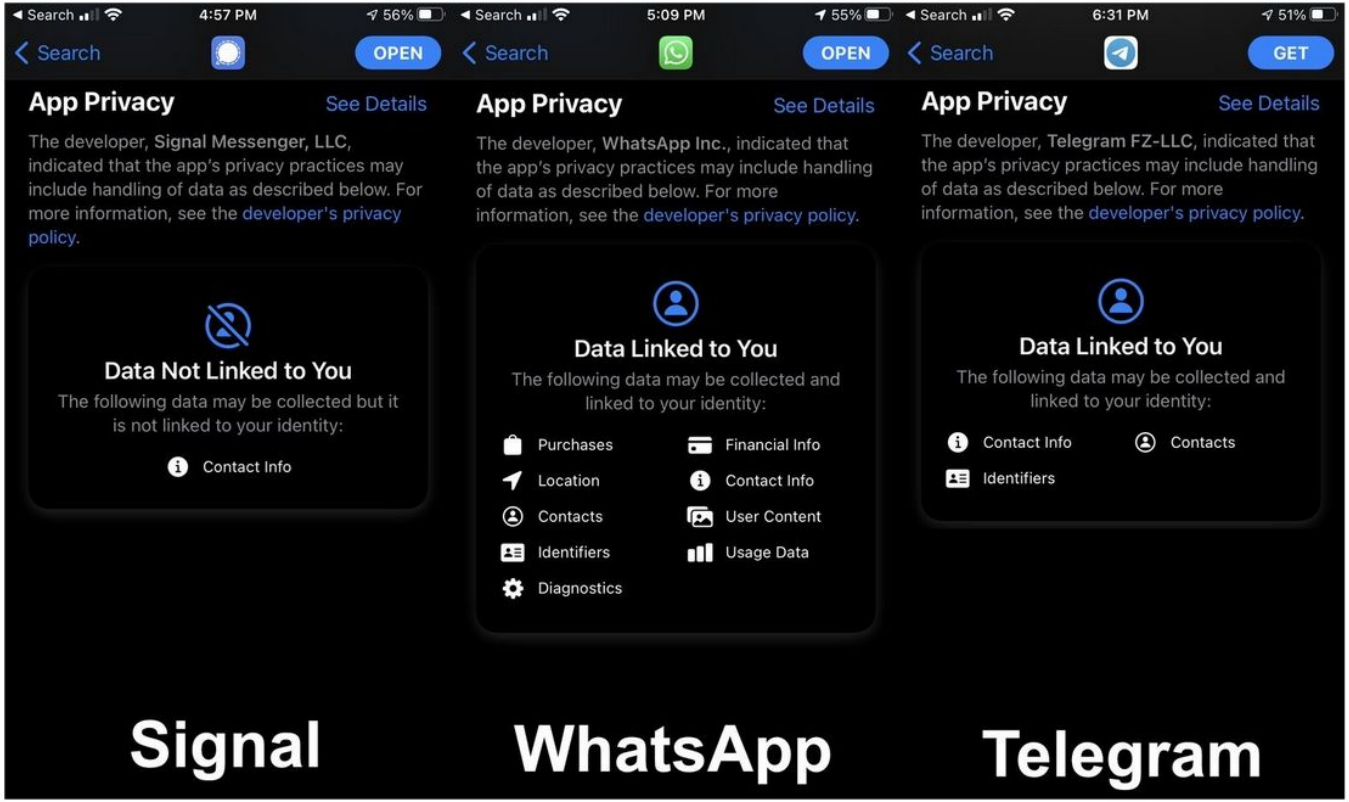


Riassunto Protezione Metadati

Quali metadati vengono protetti dalle applicazioni

		solo chat segrete	
localizzazione precisa e2ee	localizzazione precisa e2ee		localizzazione precisa e2ee
private contact discovery	numero non visibile (username)		
secure value recovery			
sealed sender			

Metadati Raccolti dalle Singole App



A voi la scelta!

Contatti

- Sito: Mvtinapwn.it
- Sito: Conoscerelinux.org
- Mail: mvtinapwn@gmail.com
- Facebook: facebook.com/MvtinaPwn

Fonti

Conferenza im irl | TL;DR instant messengers in real life di Cyber Saiyan (organizzatori RomHack)

- www.youtube.com/c/CyberSaiyan

Zoom End-To-End Encryption

- support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings

Secure connections: How Google Meet keeps your video conferences protected

- cloud.google.com/blog/products/g-suite/how-google-meet-keeps-video-conferences-secure

Sicurezza Microsoft Teams

- docs.microsoft.com/it-it/microsoftteams/teams-security-guide