End-to-end encrypt your Twilio Programmable Chat

Solve security and compliance issues with the Virgil Security end-to-end encryption overlay for Twilio Programmable Chat.

Virgil E3Kit — an open source framework that layers on top of your Twilio messaging functions to encrypt data before it's passed to your application or Twilio.

All encryption and decryption happens on the end user's device. Message data passes through all your application's existing systems and third party services, including the Twilio cloud, but is first encrypted using private encryption keys generated locally on the user's device. The application developer and Twilio see only scrambled jibberish and have no way to decrypt it.

Common use cases:

Mobile application with chat or data sharing

Chat within Flex contact center

In-browser chat

Secure chat alongside Twilio Video

File sharing or records syncing between any two endpoints

Healthcare applications that need to comply with HIPAA must use a two pronged approach for Twilio to be considered as a "conduit" and safe to use without a BAA:

- end-to-end encrypt user message data using E3Kit
- hard code your message data to delete from Twilio upon final delivery

How it Works:

1. Create a Twilio account and implement the Twilio Programmable Chat SDK in your application.
2. Create a Virgil Security account and layer the E3Kit end-to-end encryption SDK over your Programmable Chat.
3. Delete all Programmable Chat messages from Twilio once they are delivered to their end recipient.
4. If you need persistent message cloud storage, pass the encrypted message data to a HIPAA-compliant cloud provider (with a BAA in place). If you choose not to do this, any data will only be stored locally on the user's device and not retrievable from other devices or recoverable if the user loses their device.

Will this affect my application's user experience?

End-to-end encryption using E3Kit should be invisible to the end user. Your users will send and receive their messages they normally would.

With E3Kit, your app will pass the user's identity from Twilio to Virgil, then securely generate a private key on the user's device, look up the public keys for any recipient(s) they're sending encrypted data to, and allow the user to access their encrypted data from any device they'd like.

Will Virgil Security see my message data?

No. Virgil Security only provides encryption and decryption functions and the public key management, but does not store any private keys or handle any of the message data.

Virgil Security's services are zero-trust meaning that they do not have access to any private keys or encrypted data, nor would anyone who breached their system.

I don't know anything about security or cryptography. Can I still use E3Kit to add end-to-end encryption to my application?

Yes! E3Kit is designed for developers who don't have any background in application security or encryption. We abstract the complexity of asymmetric encryption and turn powerful encryption algorithms into a few lines of code in your app. You can follow our Twilio-specific guides to implement E3Kit on your client side and server side.

Who is Virgil Security?

Just like Twilio builds infrastructure tools for developers, **Virgil Security builds developer toolkits to make security simple in any application.** Our open source SDKs for end-to-end encryption and password protection turn complex cryptography into a few lines of code. Leave the key management to us, and focus on what you're good at. #SecuredByVirgil

Account setup, implementation and pricing are handled directly between application developer and Virgil Security. Pricing is based on number of registered end-users.

Open source SDKs available for web, iOS, Android, and IoT.

Sign up for a free account and get started with tutorials made just for Twilio developers at VirgilSecurity.com/e2eechat