Storing Encrypted Data on Secret Network

One of SecretPath's key features is the ability to use encrypted payloads to send over confidential messages to a Secret Smart contract.

SecretPath can seamlessly handle encrypted payloads, as the master gateway contract on Secret automatically decrypts the payload and hands the decrypted payload over to the target contract.

The encryption of the payload is done using theChaCha20-Poly1305 , anauthenticated encryption with additional data (AEAD) algorithm.

The key for this symmetric encryption is created by using theElliptic-curve Diffie-Hellman (ECDH) scheme, comprising of two components:

1. An extra encryption public key provided from the Secret Gateway Contract
2. A randomly created (ephemeral) encryption private key on the user side (independent of the user wallet's private key)
3.

Combining both of these keys together via the ECDH Scheme yields our encryption key, which we use to encrypt the payload with ChaCha20-Poly1305.

As a first example for this, we have used SecretPath to encrypt astring and subsequently store it in a Secret contract.

Last updated27 days ago On this page Was this helpful?Edit on GitHub Export as PDF