Storing Encrypted Data on Secret Network

Learn how to use Secret Network as the confidential computation layer of the Cosmos For any Cosmos chain, you can use encrypted payloads to execute and query confidential messages on Secret Network smart contracts.

Using our Confidential Computation Layer (CCL) SDK, you can seamlessly handle encrypted payloads, as the master gateway contract on Secret Network 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)

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 the CCL SDK to encrypt astring and subsequently store it in a Secret Network contract. Previous Usecases Next Key-Value store Developer Tutorial Last updated8 days ago