Viewing Keys

Viewing Keys

Secret Network uses the Cosmos SDK and its infrastructure which makes it so that the identity of a querier (someone requesting data) cannot be cryptographically authenticated. On public networks this might not be a problem for users as they can query data by using their public key. However, on private networks (where only the owners should have access) this is a problem. To solve this problem, viewing keys were implemented as a part of theSNIP-20 token specification.

Viewing keys act as an encrypted password for the viewing of data related to a specific smart contract and private key. The password can only be created by the private key owner, but anyone with the password who knows the accompanying public key gets access.

Creating Viewing Keys

To create a viewing key a user signs a transaction for a specific contract (ex sSCRT token), this transaction asks for a random input from which it generates a viewing key. The viewing key is saved in the contract state together with the user's public key (address). To query for private data (ex balance, history) both the viewing key and the accompanying address is required.

Anyone who knows the correct combination of key + address can view the private data without needing access to the private key of the address. Secret Network allows users to maintain control over their data and decide what is shared and with whom.

for more on info on Viewing keys check out the Development section forpermissioned viewing and the SNIP-20 specification

Last updated6 months ago On this page *Viewing Keys * Creating Viewing Keys

Was this helpful? Edit on GitHub Export as PDF