Permissioned.Sol

Permission

Used to pass both the public key and signature data within transactions

Should be used with Signature-based modifiers for access control

struct Permission { bytes32 publicKey; bytes signature; } Abstract contract that provides EIP-712 based signature verification for access control. To learn more about why this can be important, and what EIP712 is, refer to ourPermits & Access Control .

This contract should be inherited by other contracts to provide EIP-712 signature validated access control

SignerNotMessageSender

error SignerNotMessageSender() Emitted when the signer is not the message sender

SignerNotOwner

error SignerNotOwner() Emitted when the signer is not the specified owner

constructor

constructor() internal Constructor that initializes EIP712 domain separator with a name and version solhint-disable-next-line func-visibility, no-empty-blocks

onlySender

modifier onlySender(struct Permission permission) Modifier that requires the provided signature to be signed by the message sender

Parameters

Name Type Description permission struct Permission Data structure containing the public key and the signature to be verified

onlyPermitted

modifier onlyPermitted(struct Permission permission, address owner) Modifier that requires the provided signature to be signed by a specific owner address

Parameters

Name Type Description permission struct Permission Data structure containing the public key and the signature to be verified owner address The expected owner of the public key to match against the recovered signer Edit this page

Previous FHE.sol Next Fhenix Encryption UI