

TSS Signing Lifecycle

Once a group is created and becomes active,

D and E nonces

In the signing process, each member is required to have their nonces (D and E values).MsgSubmitDEs is the message for a member to send their public nonce to the chain. So, the chain can assign their nonce in the signing process.

message

DE

{ bytes pub_d =

1

[(gogoproto . casttype)

=

"github.com/bandprotocol/chain/v2/pkg/tss.Point"] ; bytes pub_e =

2

[(gogoproto . casttype)

=

"github.com/bandprotocol/chain/v2/pkg/tss.Point"] ; }

message

MsgSubmitDEs

{ option

(cosmos . msg . v1 . signer)

=

"address" ; option

(amino . name)

=

"tss/MsgSubmitDEs" ;

repeated

DE des =

1

[(gogoproto . customname)

=

"DEs" ,

(gogoproto . nullable)

=

false] ; string address =

2

[(cosmos_proto . scalar)

=

"cosmos.AddressString"]; } [Previous BandChain TSS Group Next Requesting a TSS Signature](#)