Key Generation

Key generation system

Description:

+ The user set the total number of parties n and the threshold t.
+ The admin account generates shares of the private key x based on Shamir's Secret Sharing.

+ The admin account send shares to n parties.

+ Each party save the partial private key locally.

Sign up

Description:

+ Set the total number of parties and the threshold.

+ Input the name and email address of each party.

Key Distribution

Description:

+ Generate partial private keys based on Shamir's Secret Sharing.
+ Send secret shares to each party by email.

Key Reconstruction

Key reconstruction system

Description:

+ The system broadcasts a link to each party by email.

+ Each party enters the partial key in the link.

+ When enough parties provide their secret shares, the system will automatically reconstruct the original private key in the backend.