

Key Generation

The diagram illustrates the Key Generation process in a 3-party threshold scheme. It involves three main entities: a Wealth Manager (green), a Key Shard Server (blue), and a Client (yellow). The process is as follows:

- Generate Share:** Each entity generates a share of the key. The Wealth Manager and Client generate their shares, while the Key Shard Server generates a share and stores it.
- Verify Share:** Each entity verifies the share generated by the other two parties. This is represented by dashed arrows labeled "verify share" pointing from each entity to the other two.
- Derive Public Key:** The three key shards are combined to derive the public key. This is represented by a solid arrow labeled "derive public key" pointing from the three key shards to the final public key.
- Generate Address:** The public key is used to generate an address. This is represented by a solid arrow labeled "generate address" pointing from the public key to the final address.

The final output is a public key and an address. The public key is shown as a blue key icon, and the address is shown as a yellow key icon.

