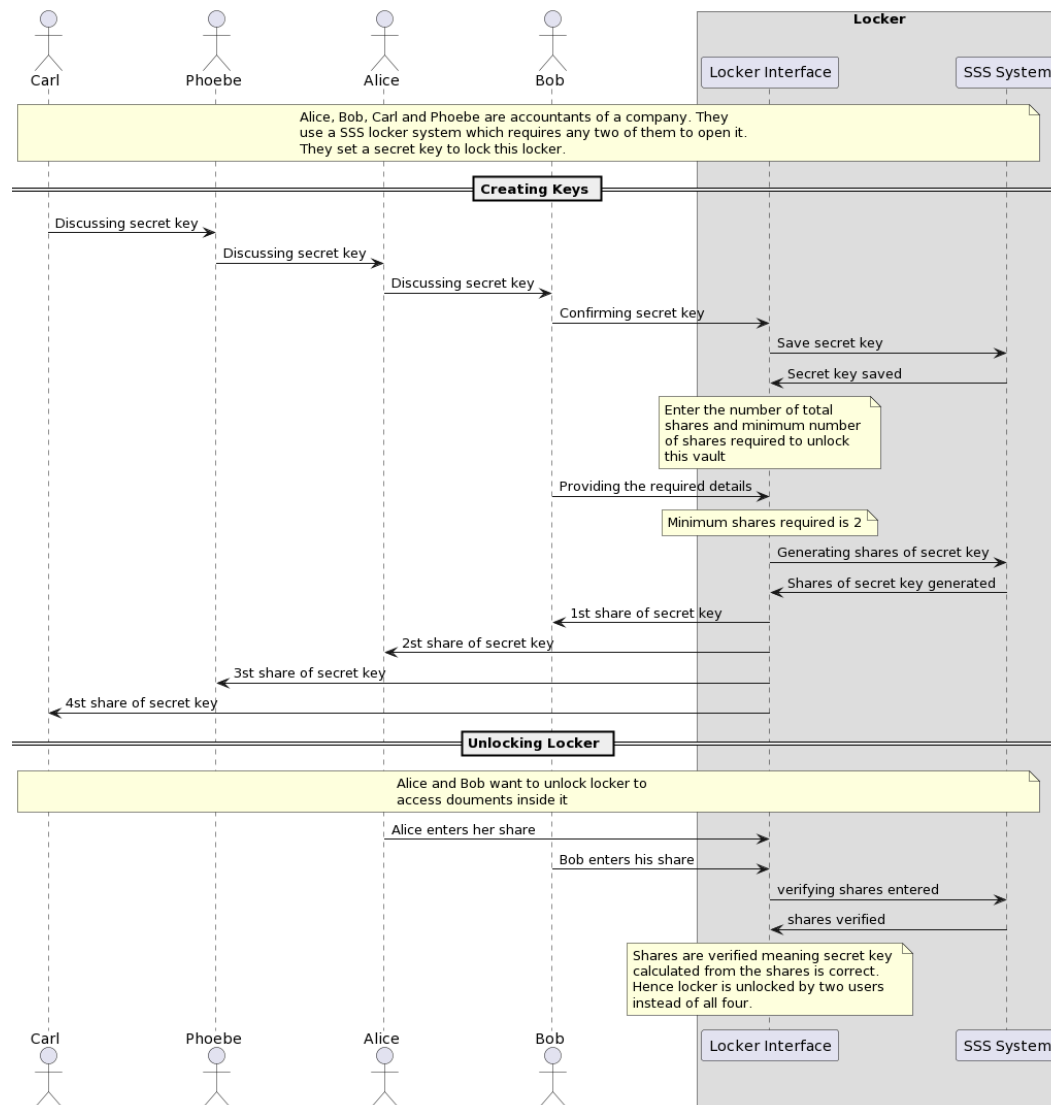# SSS Design Document

Overview:

In SSS, a secret key for any system is secured by transforming that key into multiple shared keys. Each key belongs to a different user, to get past this security; a minimum number of shared keys should be used. In this case there are 4 shares of the secret key but the required number of minimum shares is 2. This means even though there are 4 shares of the secret key, the locker can be accessed by 2 users since the minimum number of required shares are 2.

Sequence Diagram:

Class Diagram:

```
┌─────────────────────┐
│  (C) User           │
├─────────────────────┤
│  □ name             │
│  □ shakey           │
└─────────────────────┘
          │
          │
┌─────────────────────┐
│  (C)   SSS          │
├─────────────────────┤
│  □ seckey           │
│  □ tshares          │
│  □ rshares          │
├─────────────────────┤
│  ● verify()         │
│  ● genshakey()      │
└─────────────────────┘
```