JENS NEUHALFEN

SLEEP BETTER WITH CONTENT ENCRYPTION

ACCESS CONTROL

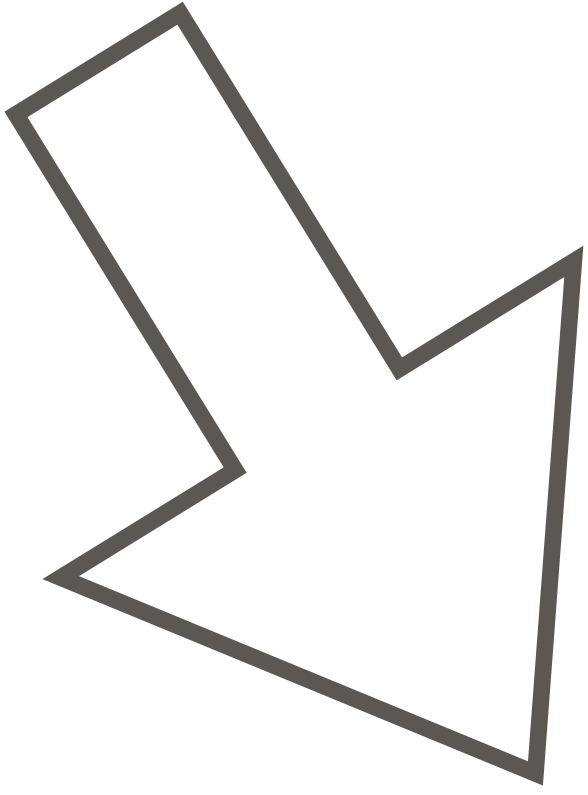
DATA

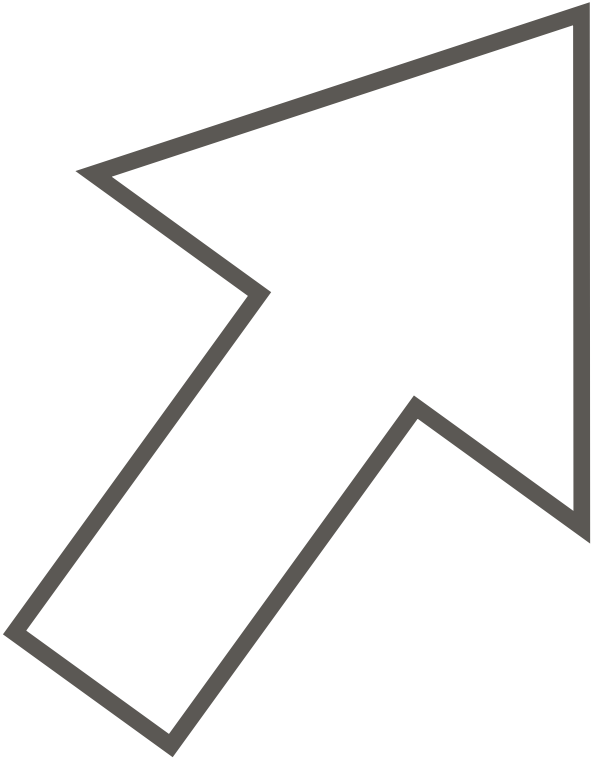
1. Alice enters her password

2. Application decrypts her strong long-term key

3. Alice now has her long-term key

Alice's long term secret key
encrypted with her password.





(3)

Alice

(1)

Alice

*****

DECOUPLE PASSWORD AND LONGTERM KEY TO ALLOW EASY PASSWORD CHANGES

ACCESS CONTROL

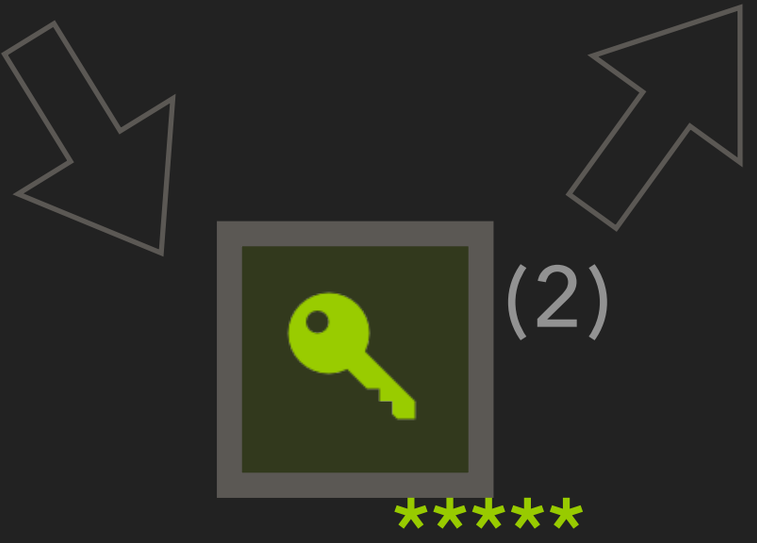
(1)

Alice

*****

(3)

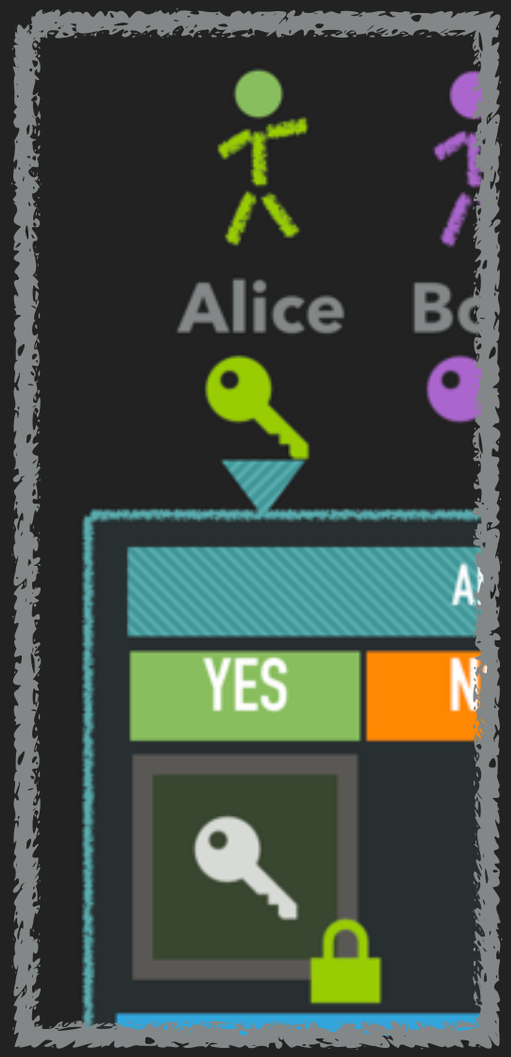
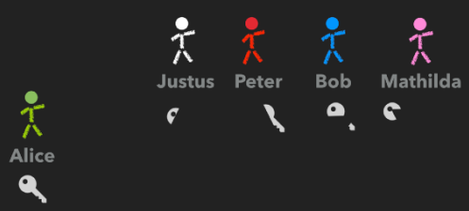
Alice



1. Alice enters her password
2. Application decrypts her strong long-term key
3. Alice now has her long-term key

Alice's long term secret key
encrypted with her password.

DECOUPLE PASSWORD AND LONGTERM KEY TO ALLOW EASY PASSWORD CHANGES

ACCESS CONTROL

Situation: