JENS NEUHALFEN

GOOD CRYPTOGRAPHY

ACCESS CONTROL

DATA

YES

NO

NO

ACL

Alice

Bob

Eve

Your application

1. Alice tries to read data

2. Application validates ACL

3. Alice is granted access

4. Alice decrypts the “data key”

5. Alice decrypts data

encrypted with

data key

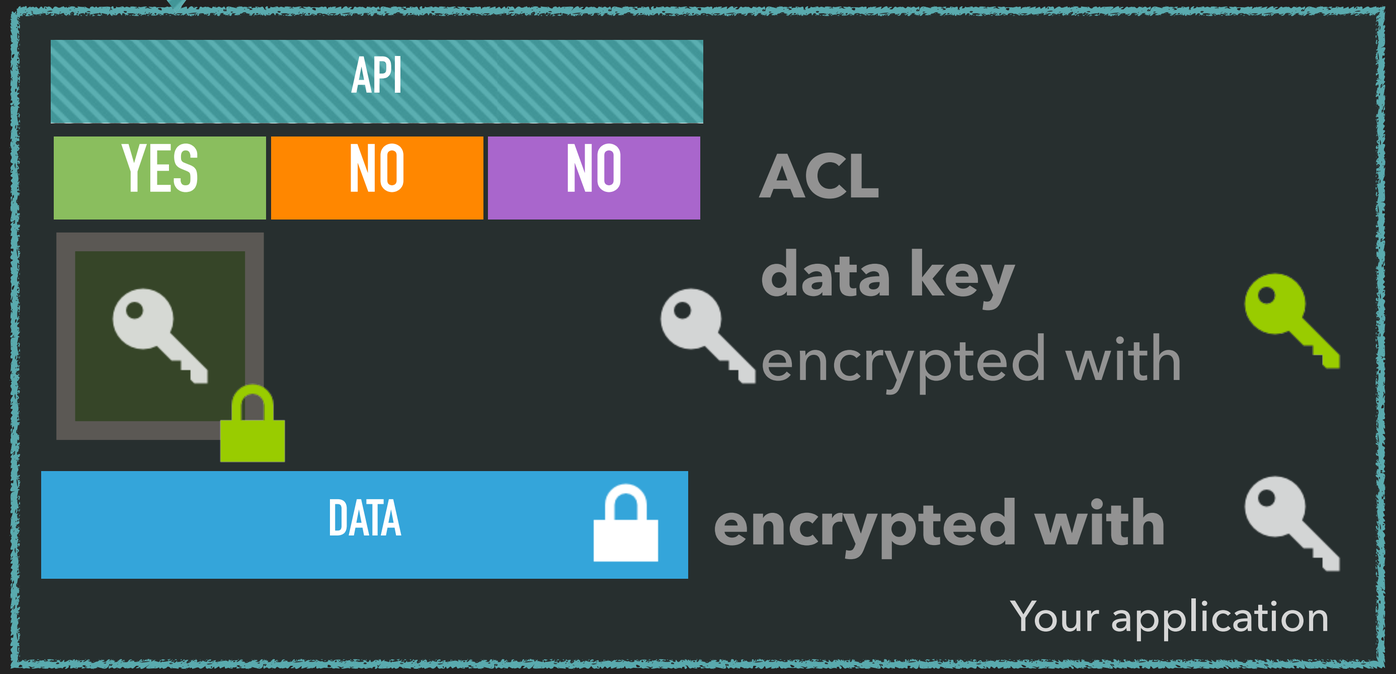
encrypted with

DATA

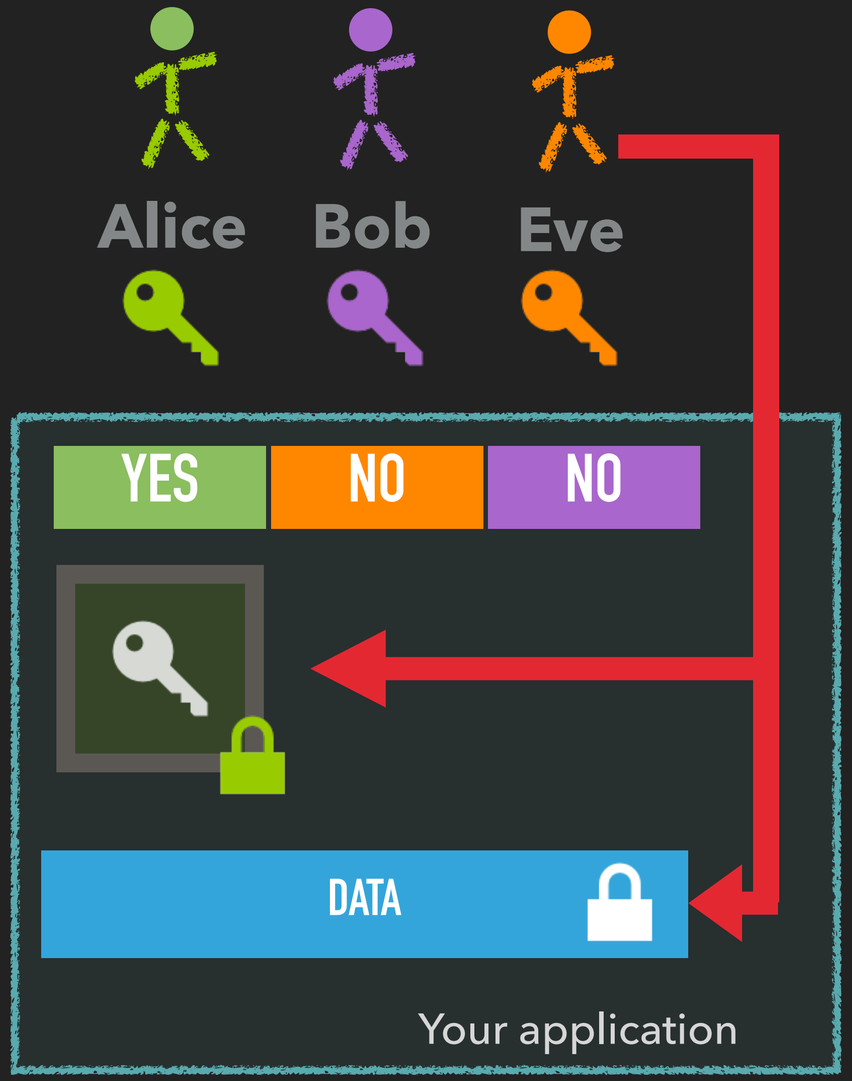
API

ACCESS CONTROL

1. Alice tries to read data
2. Application validates ACL
3. Alice is granted access
4. Alice decrypts the “data key”
5. Alice decrypts data



ACCESS CONTROL



1. Eve exploits application