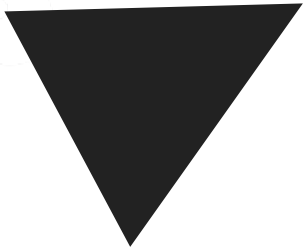
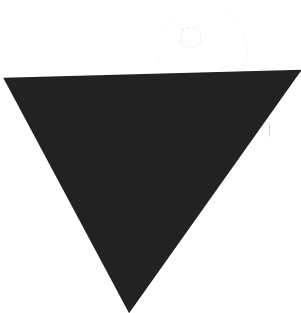
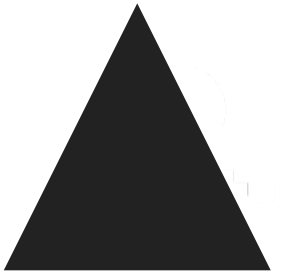


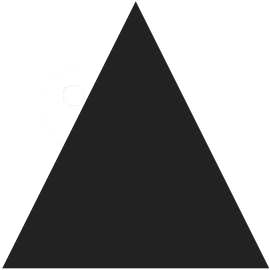


JENNER









ACCESS CONTROL



108

Problem: What happens when Alice forgets her password?

Solution: Use cryptographic secret sharing for recovery



DATA





Alice

Justus



Peter



Mathilda

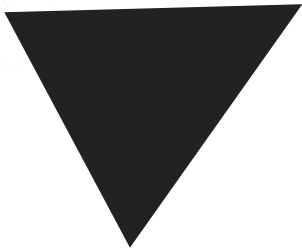


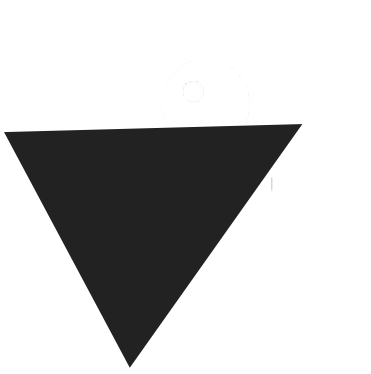
Bob

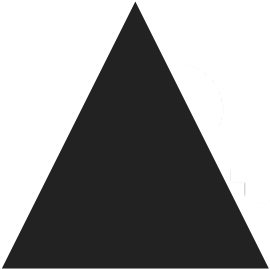


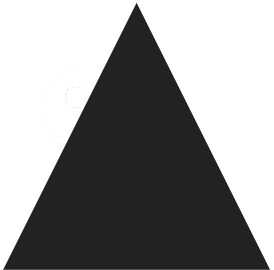
Alice will split her secret key (e.g. with Shamir) in such a way,
that any three of her four trusted friends can restore the key.

Alice trusts her friends only so far.
But she thinks it is very unlikely that
three of them conspire together
against her.









109

Problem: What happens when Alice forgets her password?

Solution: Use cryptographic sealing for recovery



Alice

Justus



Peter



Mathilda



Bob



Alice will split her secret key (e.g. with Shamir) in such a way,

that any three of her four trusted friends can restore the key.



Secret sharing ("t out of n") share a secret

such, that the secret can be restored with

without a single point of trust (failure).

This can be used for secret recovery

any of the n (here 4) parts.



