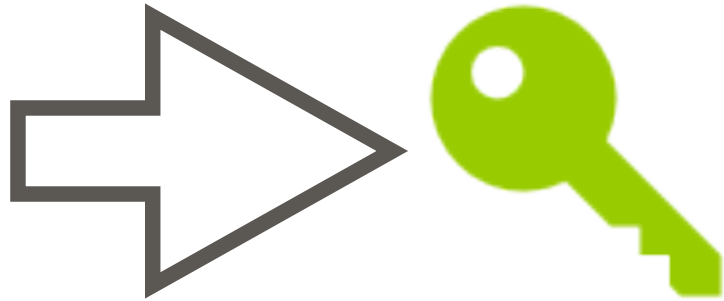
JENS NEUHALFEN

****

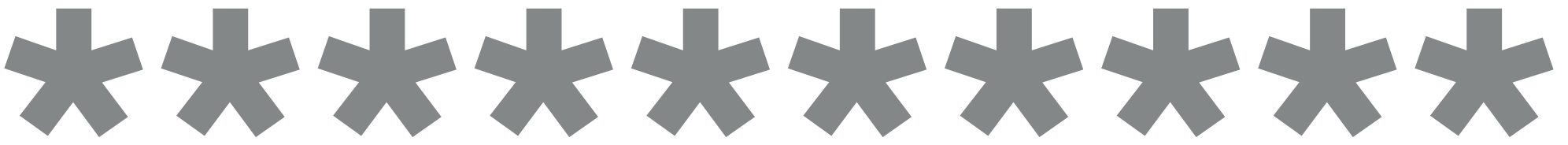


FROM PASSWORD TO KEY

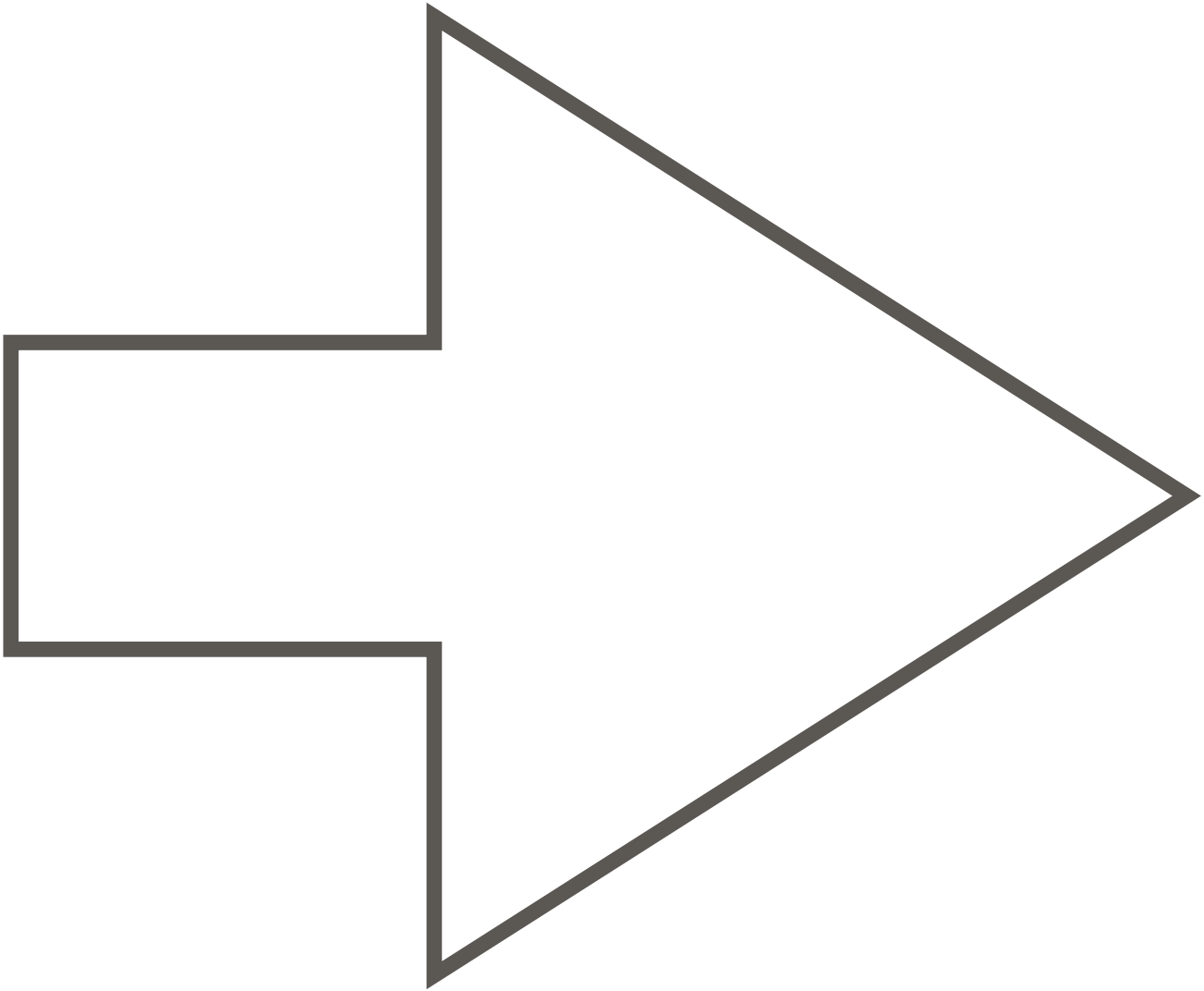
SLEEP BETTER WITH CONTENT ENCRYPTION

58

128 bit key



password



- A *random* password has
  ~ 6 bits per character (*)
- A 128 bit key needs >= 21 character passwords

(*) a-zA-Z0-9 –> ~64 different values per character (2^6). A 128 bit passwords must be >= 21 characters long (128/6)

Secure passwords are *very* long

FROM PASSWORD TO KEY

****

****

password

128 bit key

- A *random* password has
  ~ 6 bits per character (*)
- A 128 bit key needs >= 21 character passwords

Secure passwords are *very* long

(*) a-zA-Z0-9 –> ~64 different values per character (2^6). A 128 bit passwords must be >= 21 characters long (128/6)

FROM PASSWORD TO KEY

****

****

password

128 bit key

- `aw92SDAVglkqusabvgw38`
  - 128 bit
- `3o8uGsdA`
  - 8 chars, 48 bit (cracked in hours to days)