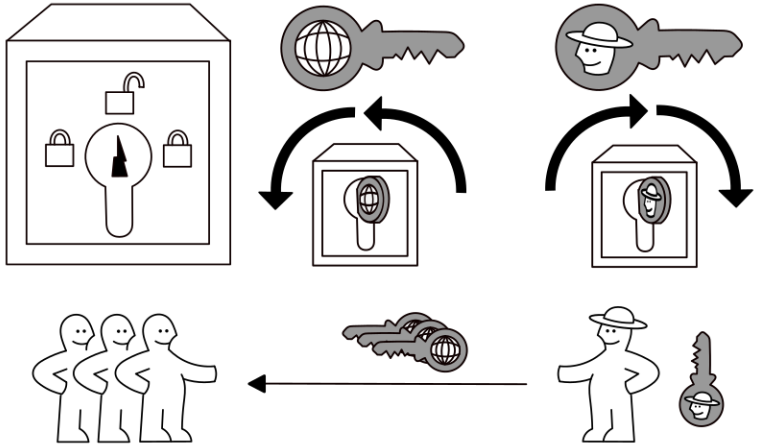
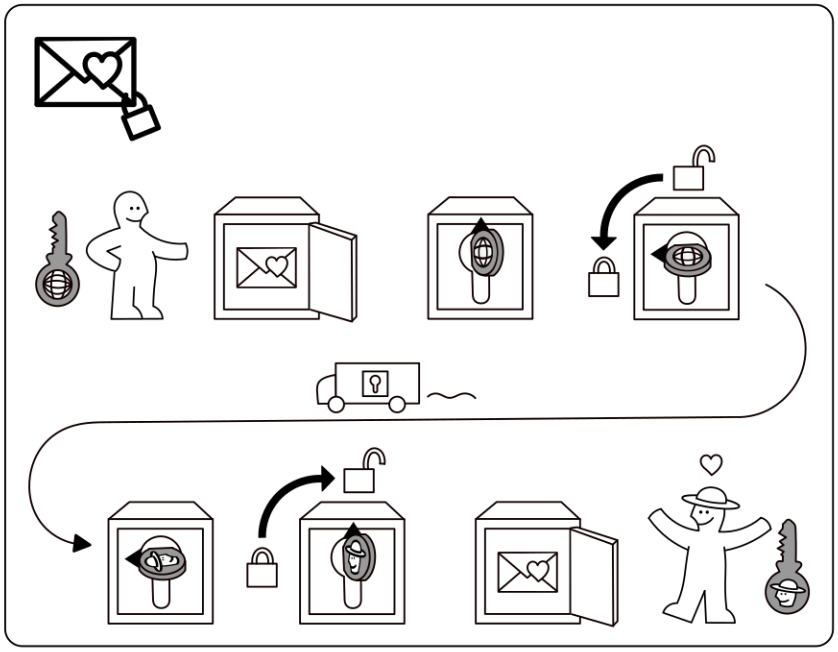
UPPSALA
UNIVERSITET

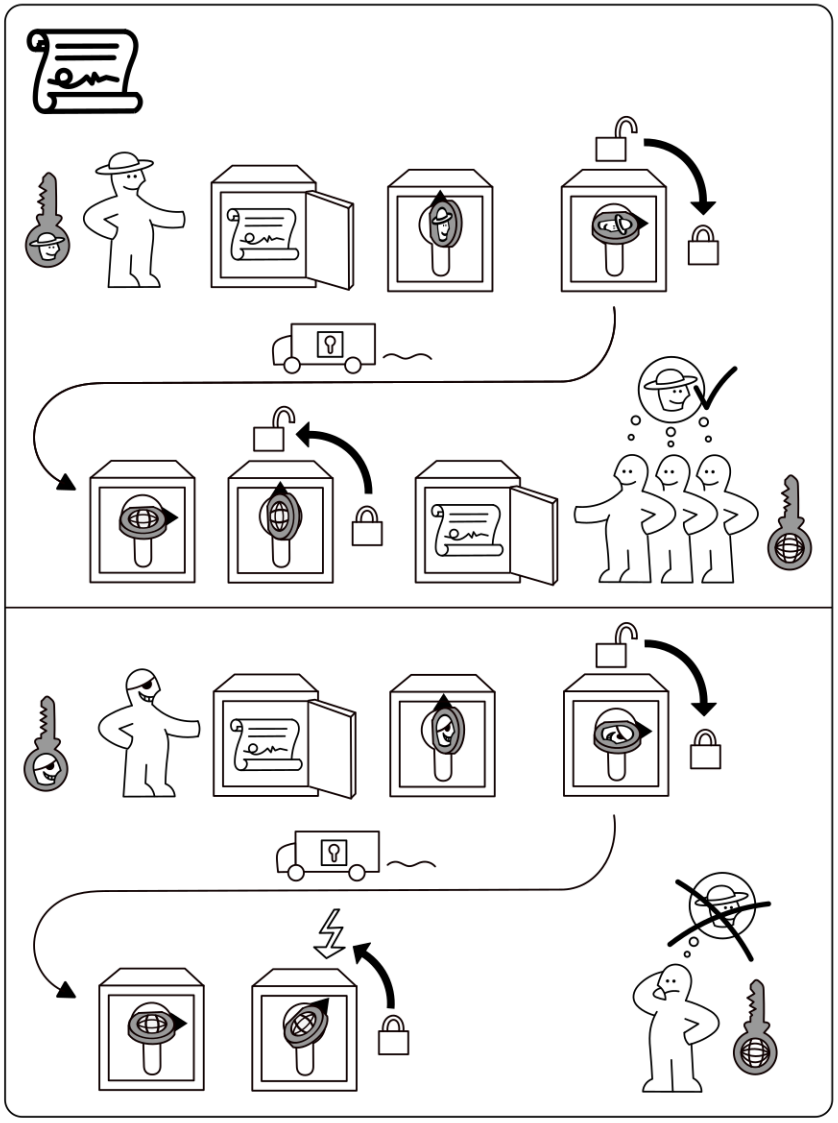
PUBLIK KEY KRYPTO

idea-instructions.com/public-key/
v1.1, CC by-nc-sa 4.0

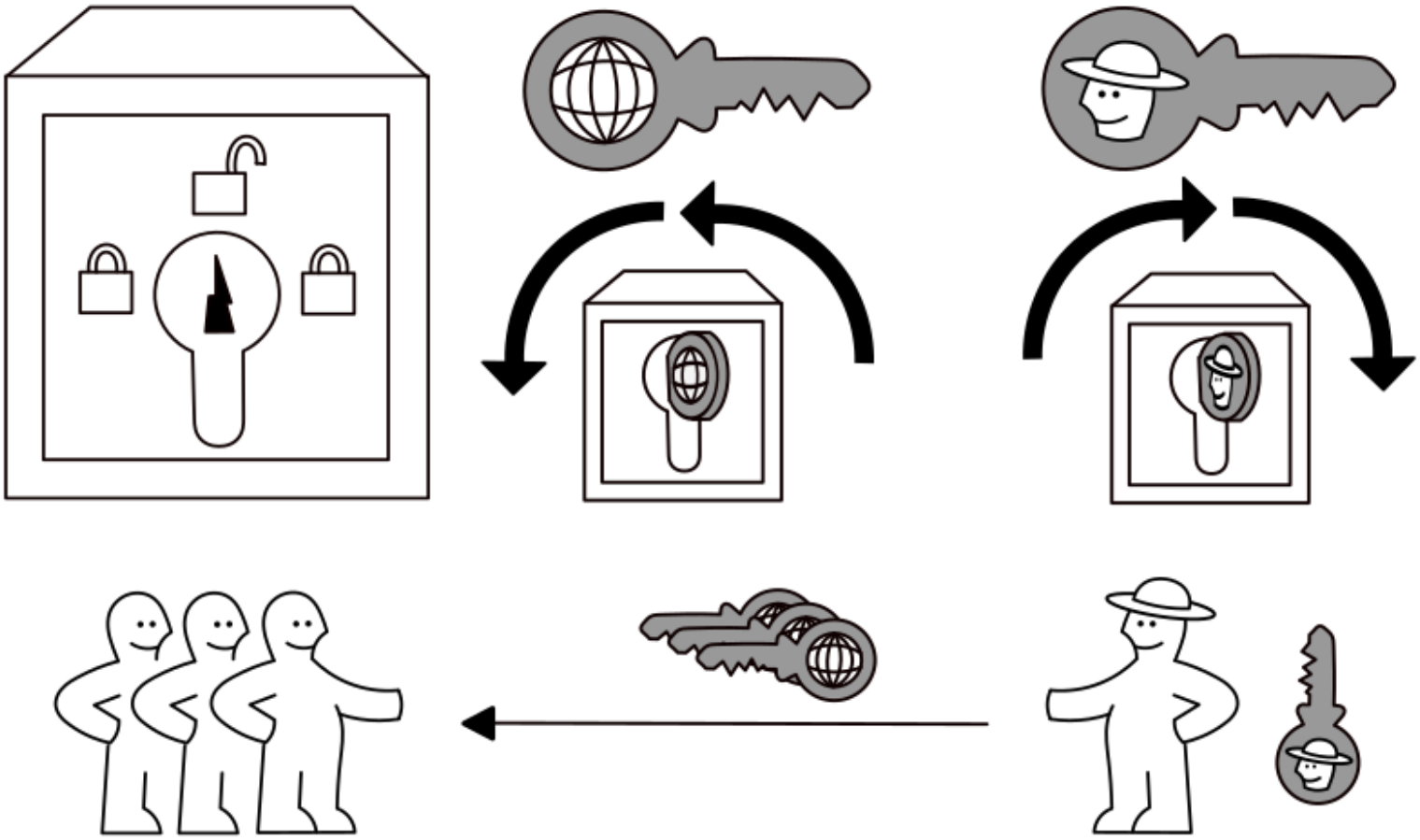
IDEA

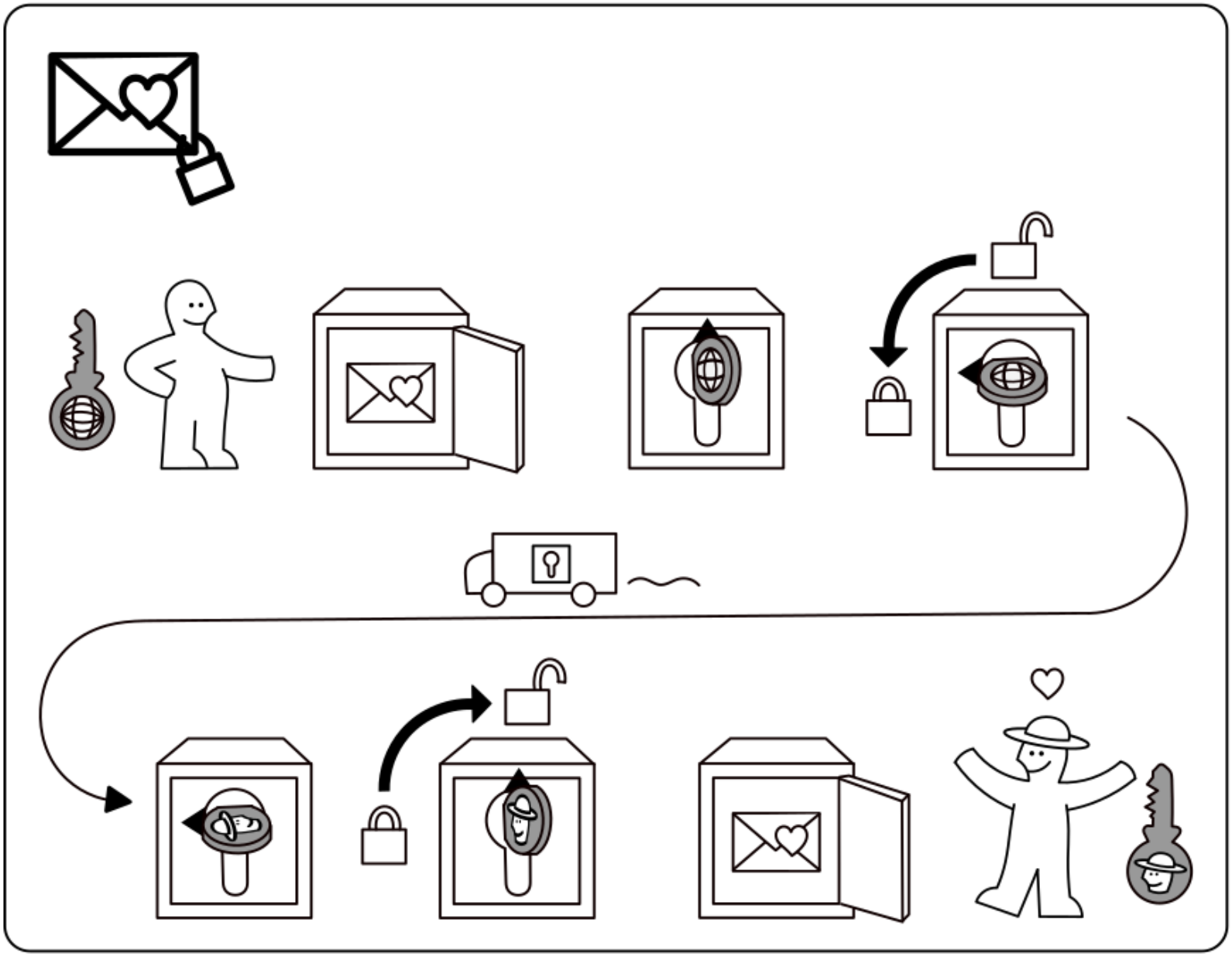


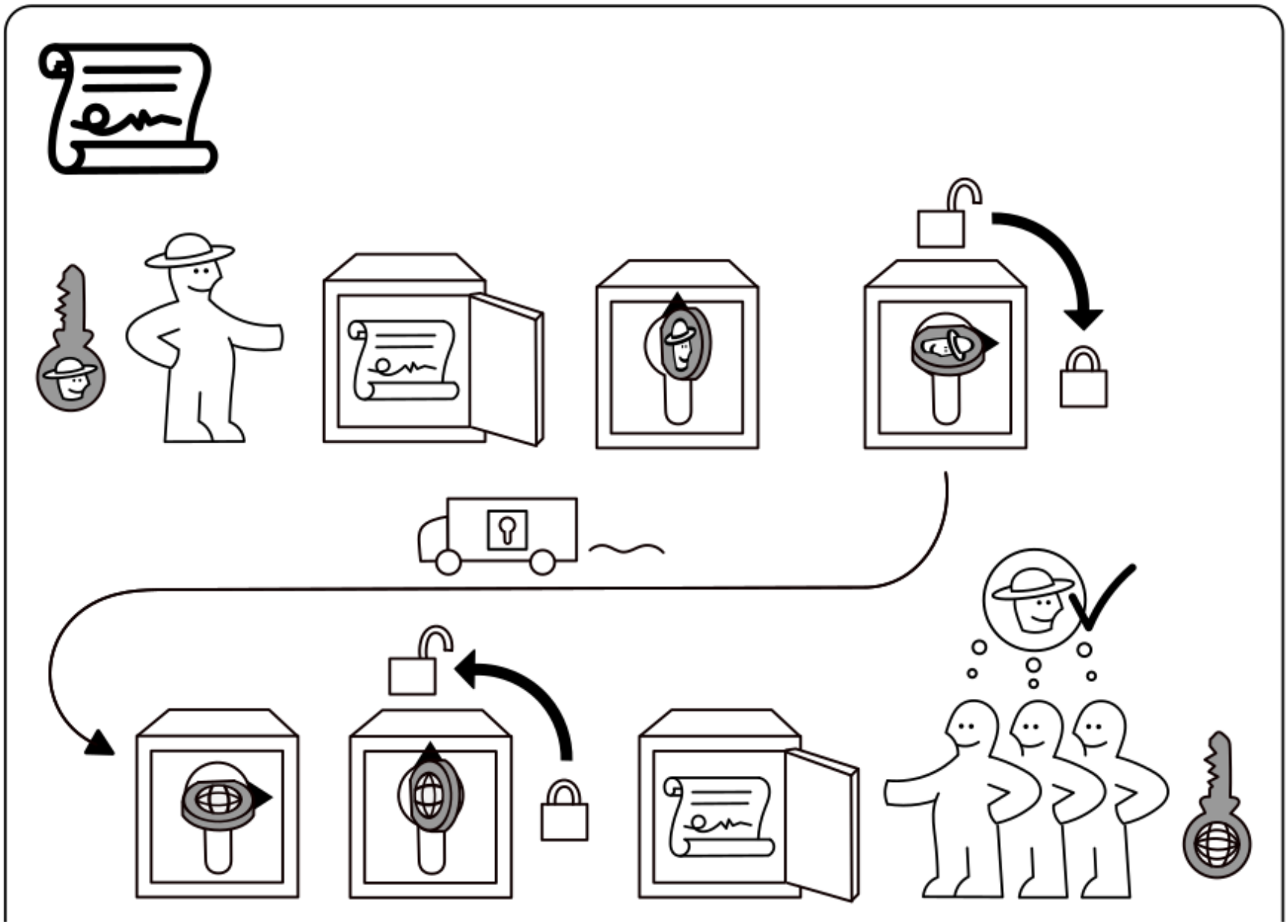


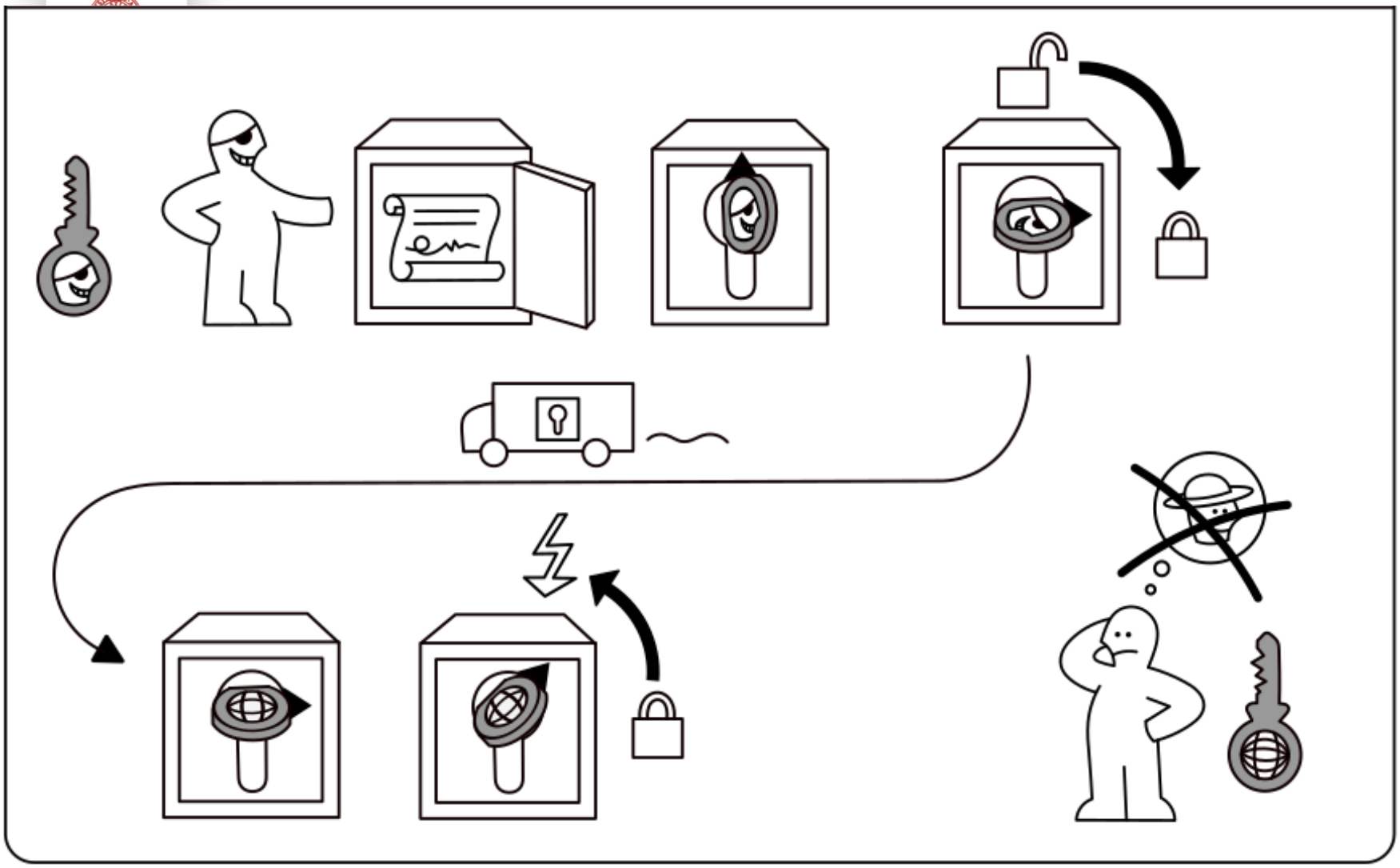


PUBLIK KEY KRYPTO









UPPSALA UNIVERSITET

Distribution av publika nycklar

- En nyckels äkthet bekräftas av ett **certifikat**
  - Digitalt signerad av en **CA (Certificate Authority)**
  - Verifieras med CA:ns publika nyckel

- Men hur vet vi att CA:ns publika nyckel är korrekt?

UPPSALA UNIVERSITET

“Chain of trust”

- Någonstans måste vi ha en nyckel vi litar på
- Denna kan användas för att bekräfta en annan nyckel…
- ...som i sin tur kan bekräfta en annan nyckel...
- ...som i sin tur kan bekräfta ytterligare en nyckel...
- ...osv.

UPPSALA UNIVERSITET

“Chain of trust”

- **Någonstans måste vi ha en nyckel vi litar på**
- Denna kan användas att bekräfta en annan nyckel…
- ...som i si nyckel...
- ...som i sin tur kan bekräfta ytterligare en nyckel...
- ...osv.

Hur? Var?

UPPSALA UNIVERSITET

Don’t panic!

- Någon har redan tänkt på detta!
  - Er datortillverkare
  - Företaget/organisationen bakom er webbläsare
  - …

UPPSALA UNIVERSITET

Self-authentication

- När man utfärdar sina egna certifikat
  - Lite som att designa sitt eget körkort!

KÖRKORT NORRLAND

1. NORDÈN
2. LARS-ÅKE FANTOMEN
3. 31.09.1970
4. 25.07.2099
5. 700931-1234

UPPSALA UNIVERSITET

Saker att vara medveten om

- Det finns en “chain of trust”
- En del försöker undvika denna
  - För att spara pengar
  - Omedvetenhet
  - För att göra något dumt
- De flesta användare är omedvetna om detta
  - Godtar snällt alla frågor om man litar på certifikat