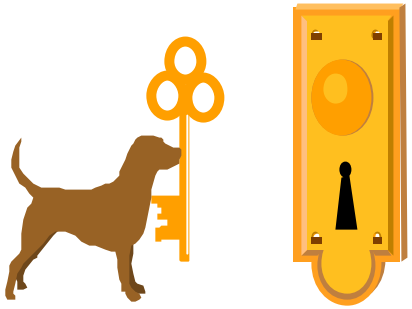
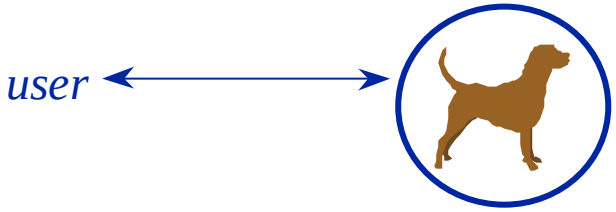
PUP security

Will Harwood

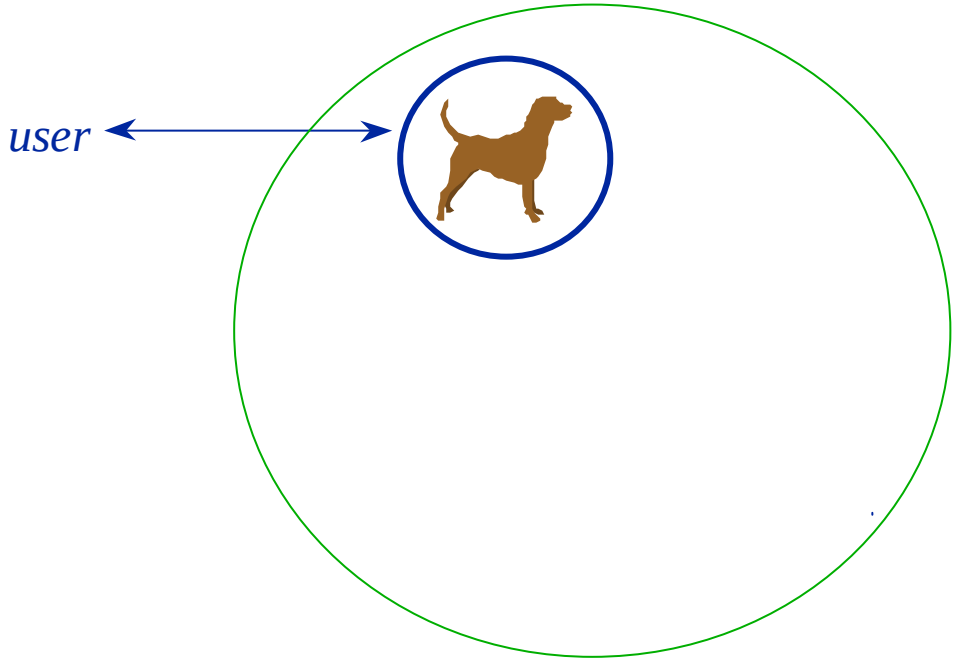
Security

- Authenticity
- Privacy
- Anonymity
- Delegation
- Non Repudiation

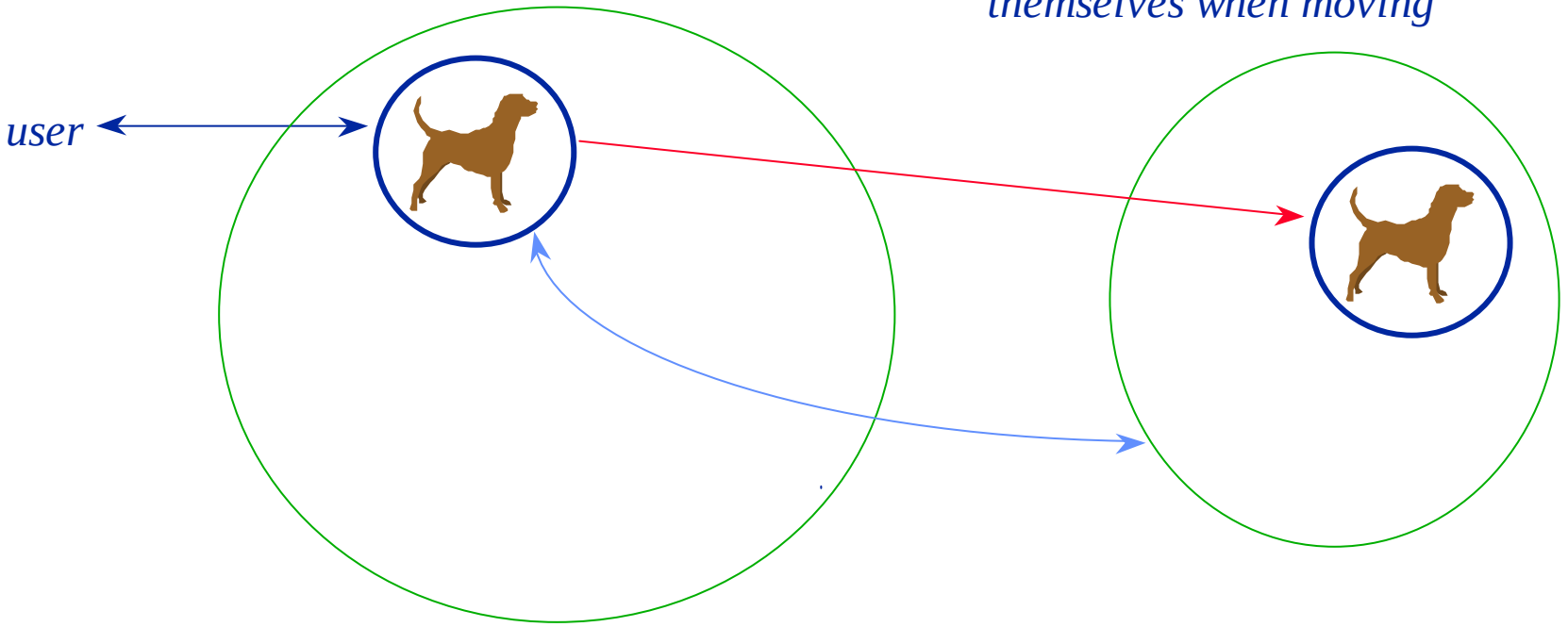


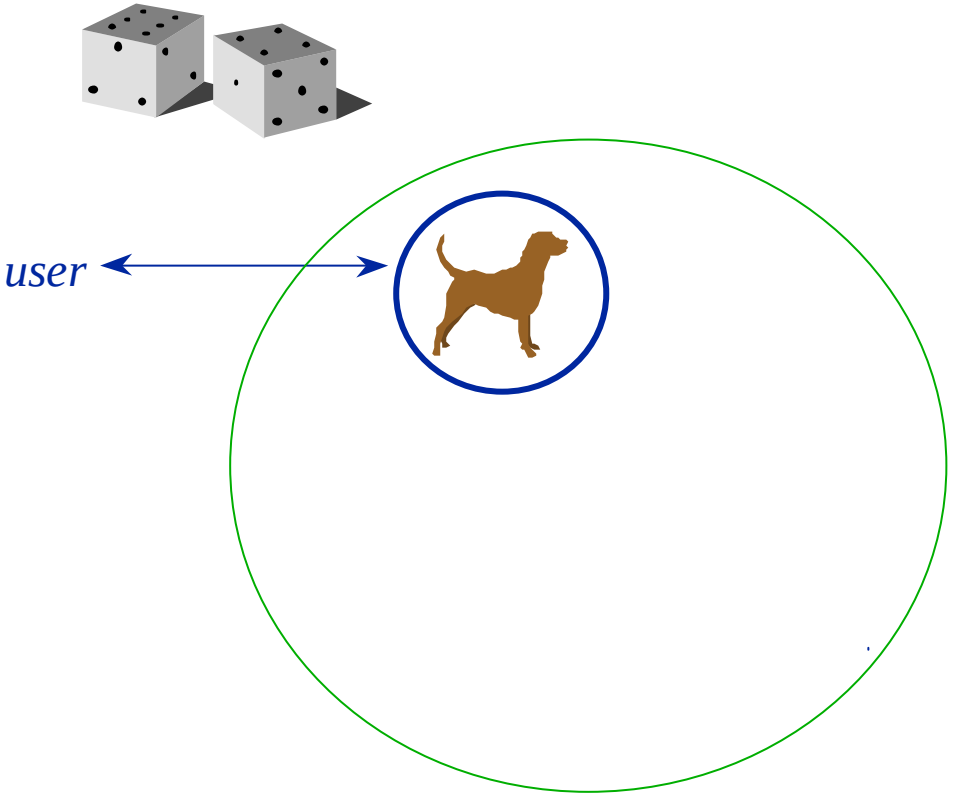

user

PUPs must be protected

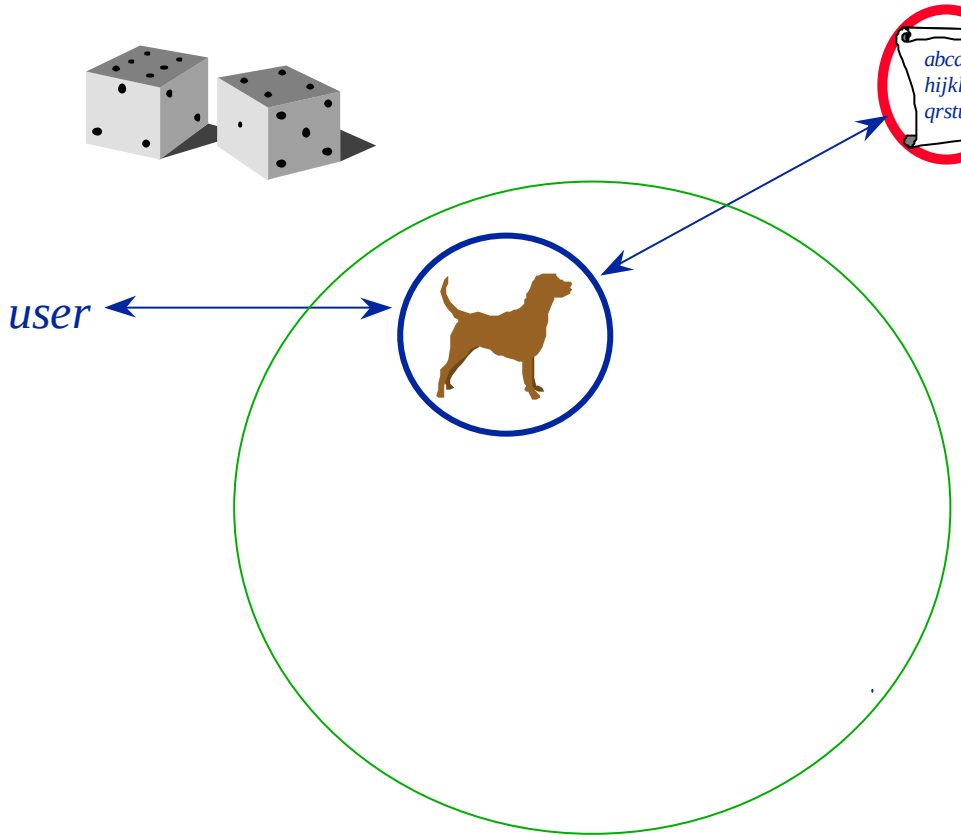


PUPs must be protect themselves when moving

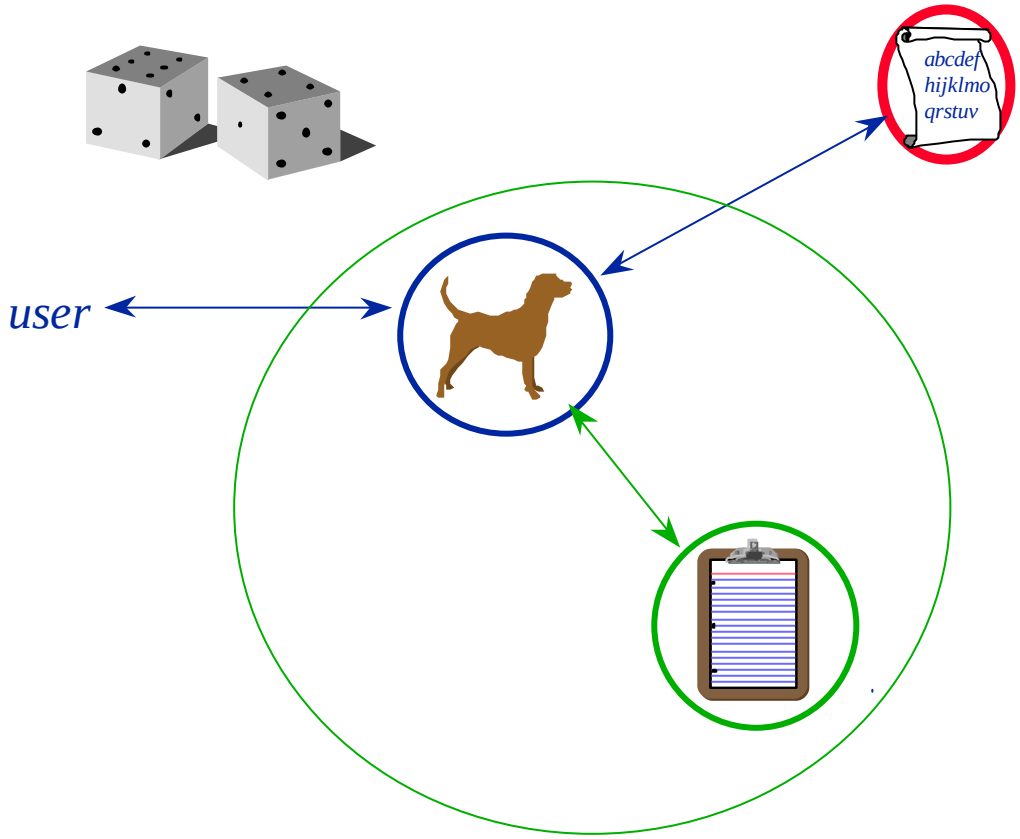




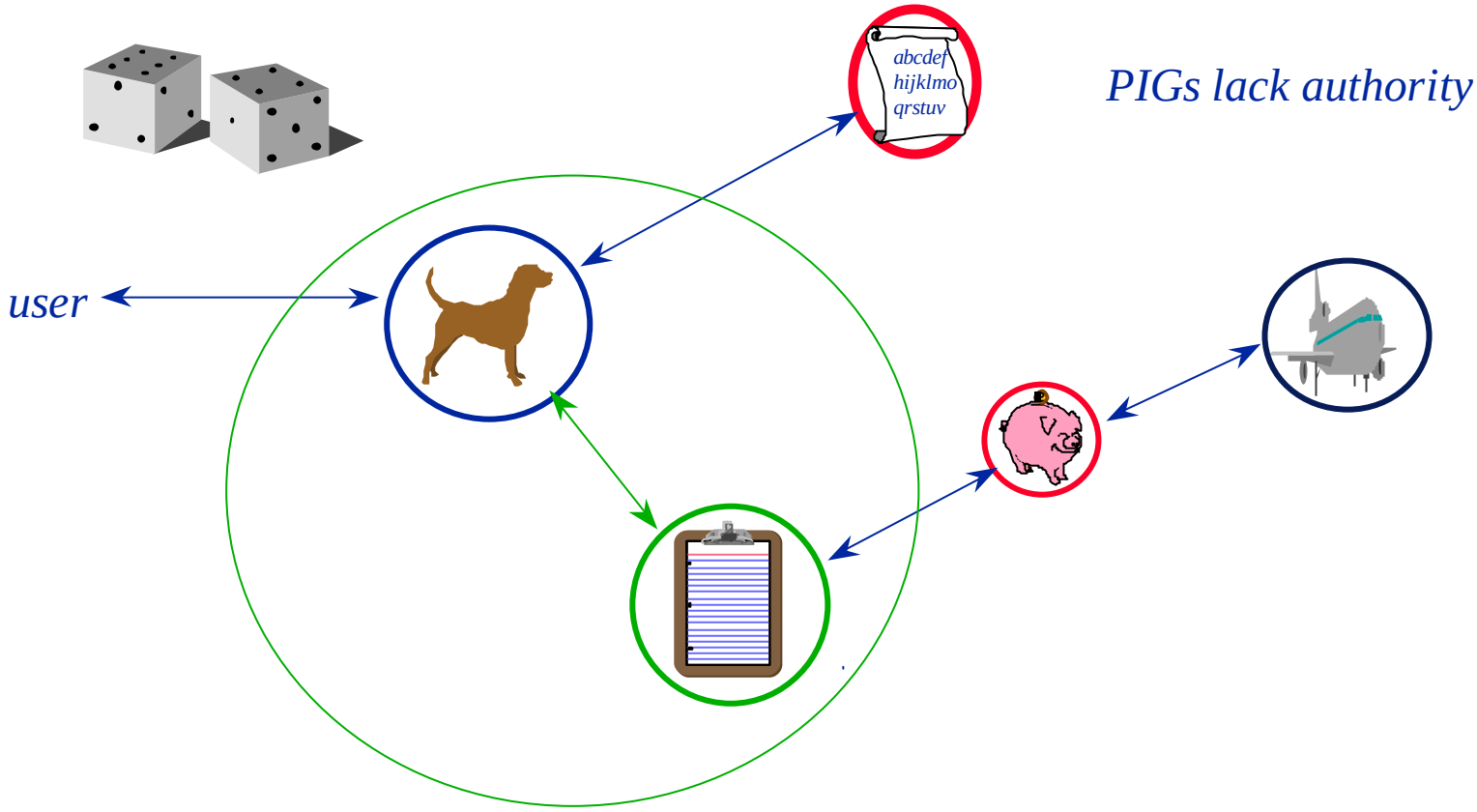
Users must be authenticated



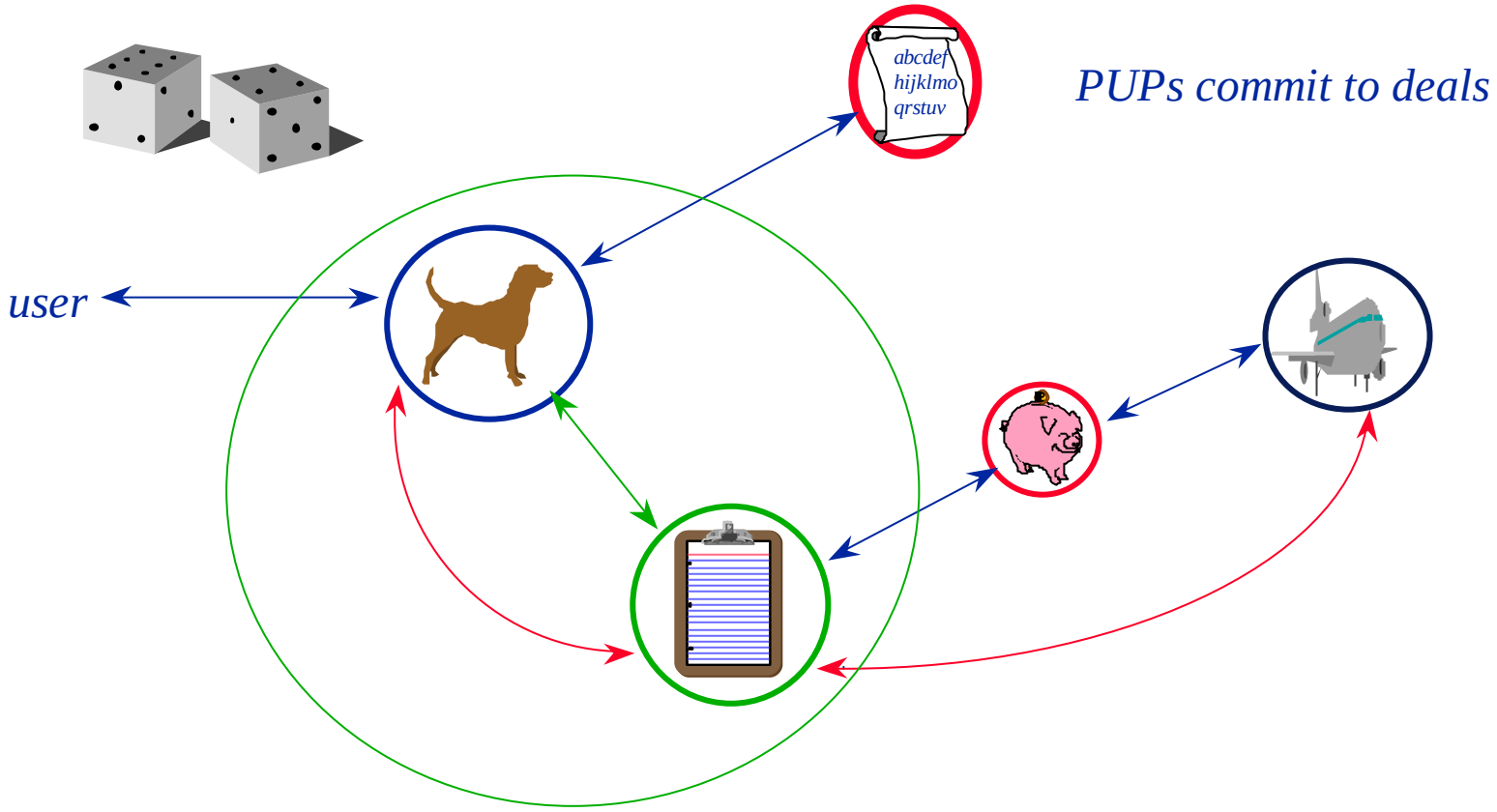
A PUP may protect data in public space



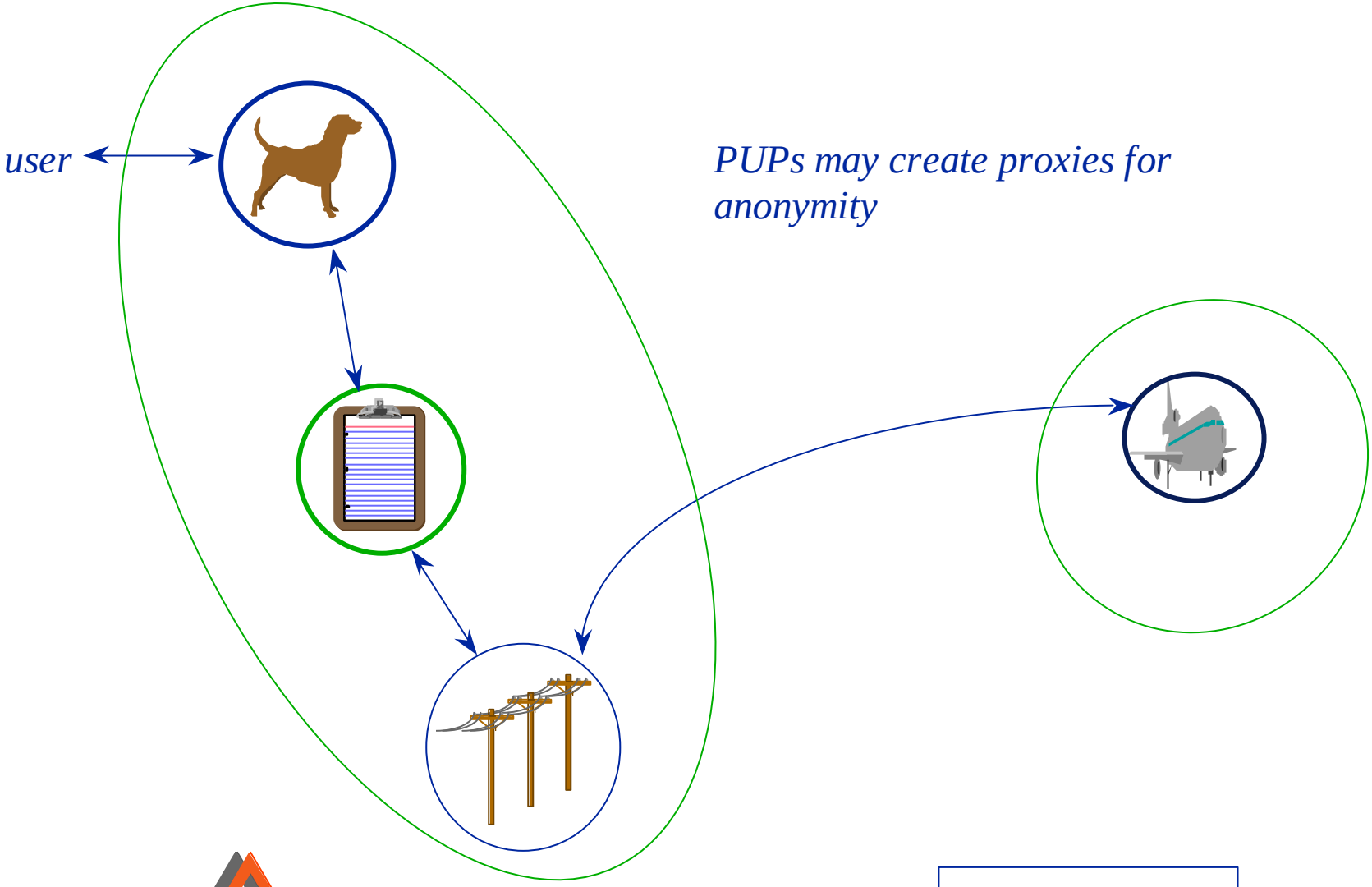
A PUP may delegate authority

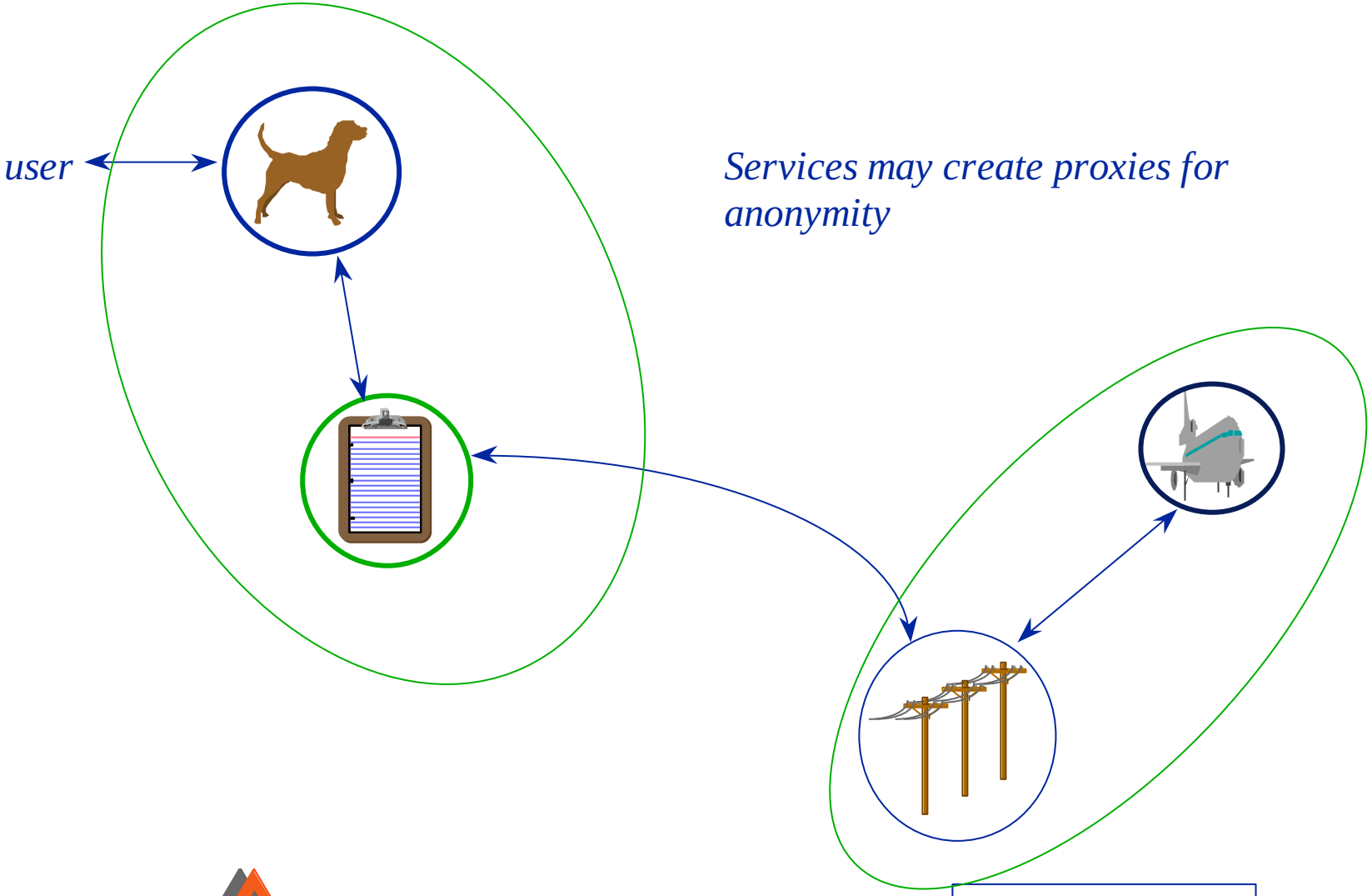


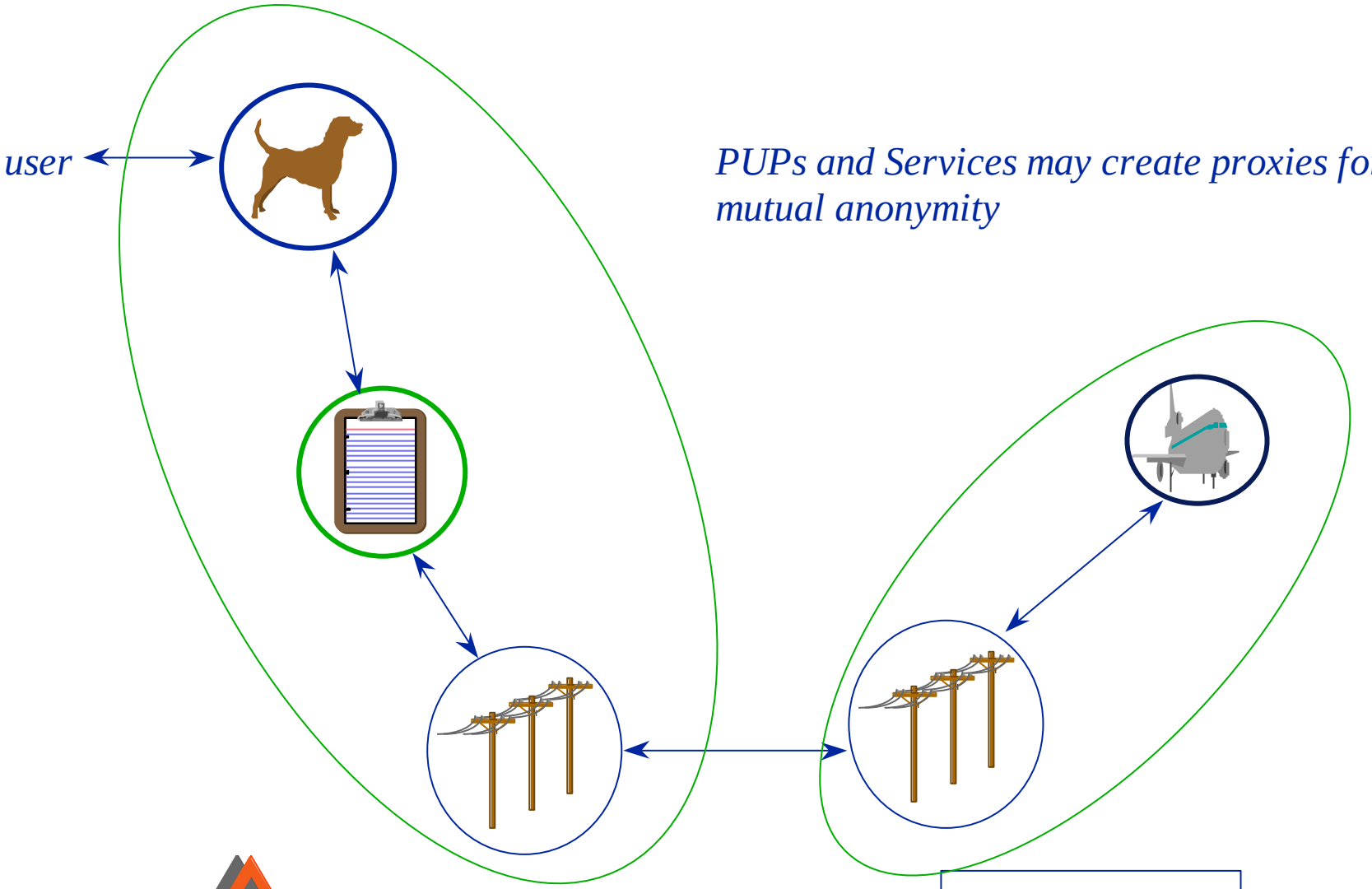
PIGs lack authority



PUPs commit to deals


user
PUPs may create proxies for anonymity


user
Services may create proxies for anonymity


user
PUPs and Services may create proxies for mutual anonymity

Authentication

- Users
  - Multiple Modalities
  - Scaleable Risk
- PUPS
  - need to authenticate their location
- Services

Privacy

- PUPs internal data
  - need to protect PUPs from disection
- User data space
  - not all user data is in a PUP
- Communication
  - User to PUP
  - PUP to TA, PIG & Service ...

Delegation & Non Repudiation

- PUPs may delegate authority to TA’s
- Users cannot repudiate deals done by PUPs
- PUPs cannot repudiate deals done by TA’s
- Service cannot repudiate deal offered

Questions

- Audit?
  - users, services, network providers
- Other notions of security?
- Do users want agents to have authority?
- Are agents actions legally binding?
- What happens at international boundaries?
- Are there valid, legal uses for double blind dealing?