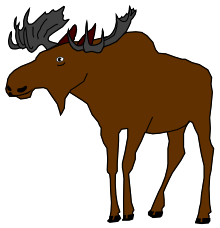
Decentralized Public-Key infrastructure

DPKI

Erik Andersen

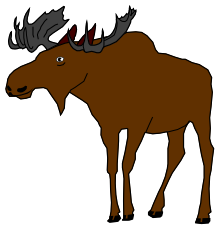
era@x500.eu



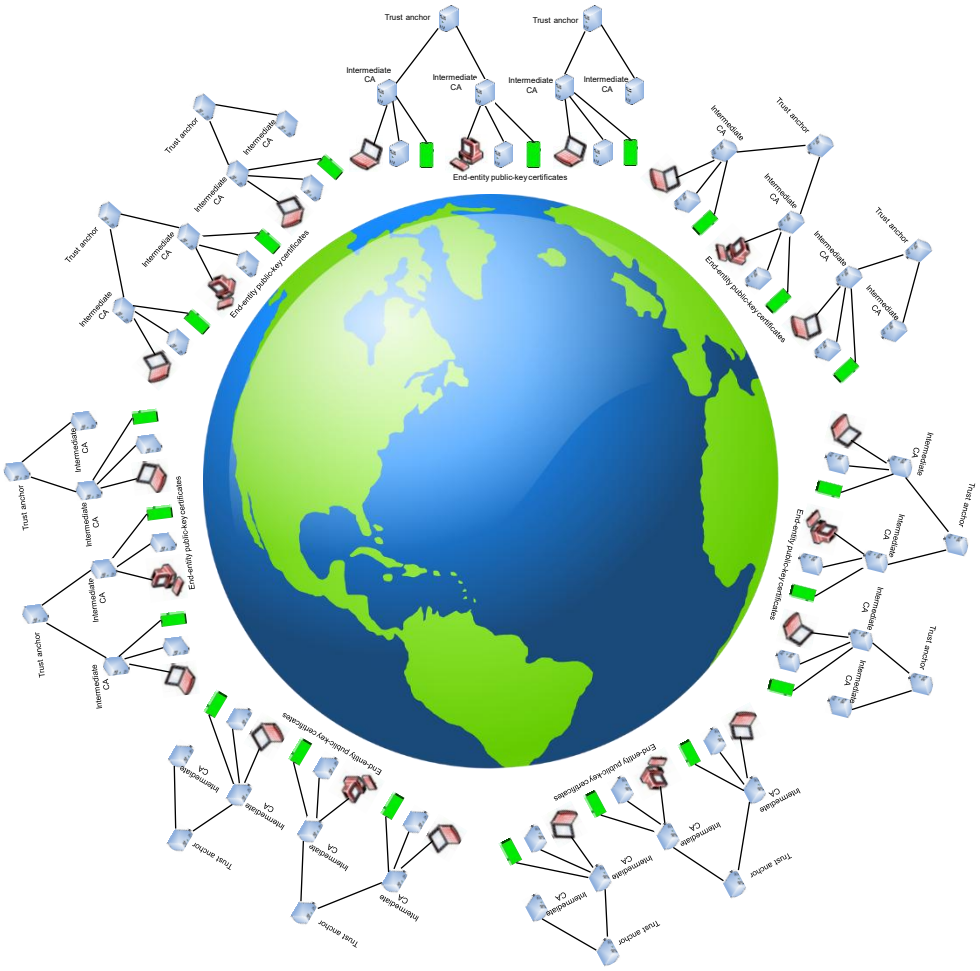
Public-key infrastructure (PKI)

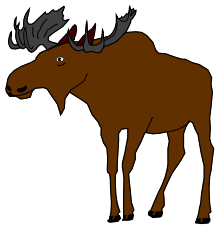
PKI is about:

Trust,
Identity
&
Privilege



A world-wide federated PKI





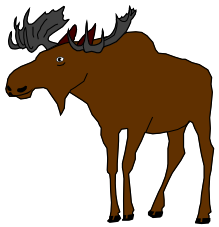
Trust by consensus

It seems problematic to create a world-wide federated PKI having world-wide trust using current PKI trust model.

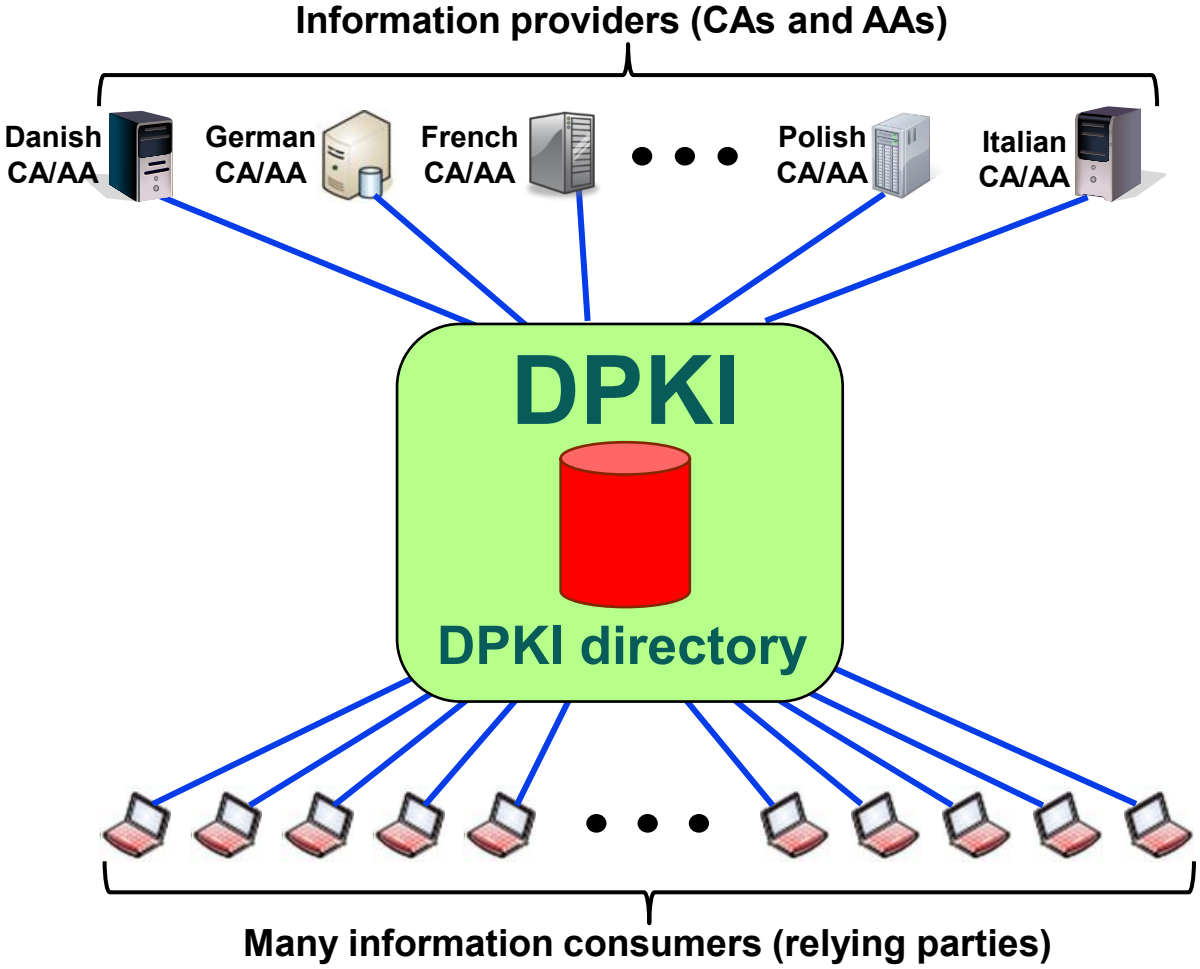
A PKI where trust is obtained by **consensus**

PKI domains federated using blockchain technology

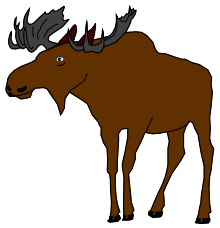
Decentralized public-key infrastructure (DPKI)



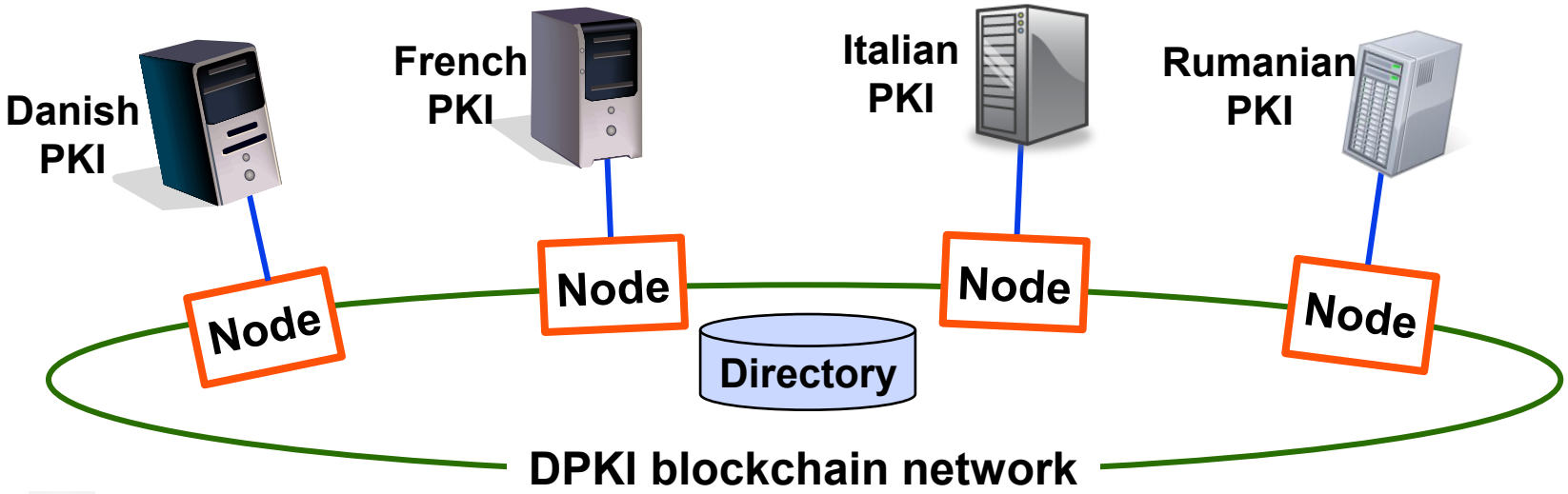
DPKI information providers and consumers



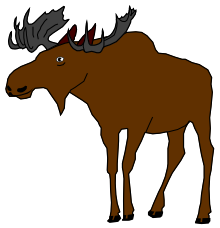
Different from other blockchain platforms: No interaction between service providers



Decentralized Public-Key Infrastructure interconnecting country PKIs

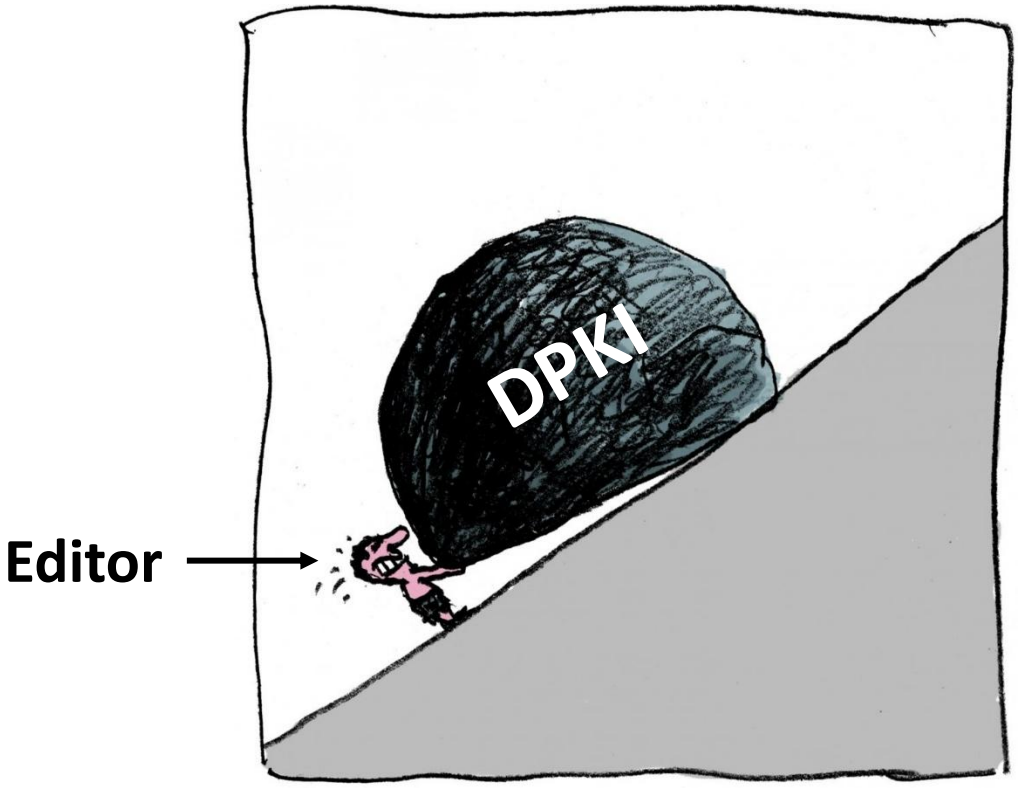


- Trust by consensus
- DPKI interconnect national PKIs e.g., for support of single market
- The concept of PKI is not changed
- PKI information (certificates and status) globally available by a DPKI directory part beginning of the ledger
- All PKI information in the DPKI directory validated and genuine
- Migration tools for cryptographic algorithm
- Some harmonisation of participating PKIs may be necessary



DPKI directory

- Directory described in terms of the X.500 directory specifications
- Easy mapping to LDAP
- Holds information about certificates (public-key and attribute certificates) and their status
- Tight specification to ensure that the DIT has exactly the same structure in all nodes



END