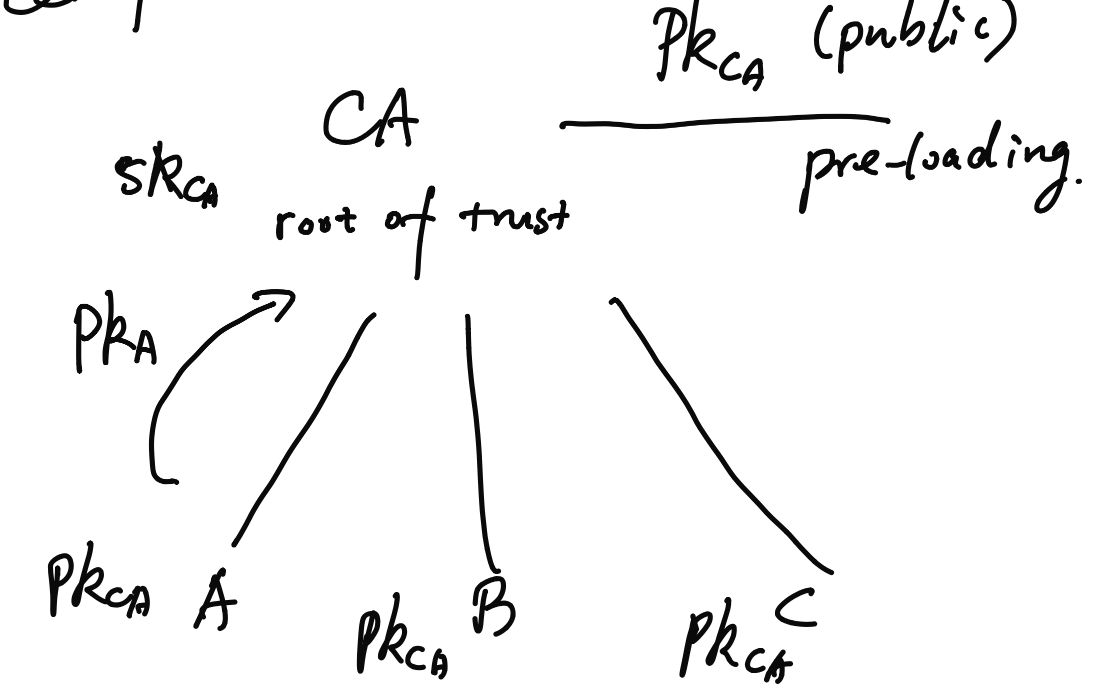
ECE 471/571 PKI

certificate



user A generates sk_A, pk_A.
gives pk_A to CA
CA sign pk_A.

$$S = sig_{sk_{CA}}(\underset{\cdots}{ID_A} \| \underset{\cdots}{pk_A})$$

$$cert_A = (ID_A \| pk_A \| S) \| \text{exp. time.}$$

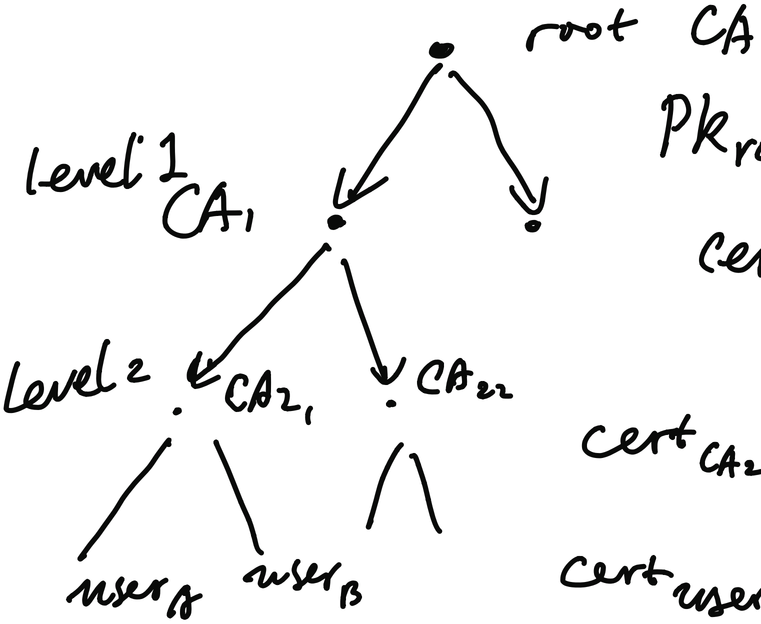
Bob receive $cert_A$

verify: $\underline{ver_{pk_{CA}}}(ID_A \| pk_A, S)$

?.

RSA. $5^e \bmod n \overset{?}{=} m$ $\overset{?}{=}$ true

Hierarchical approach



pk_{root}.

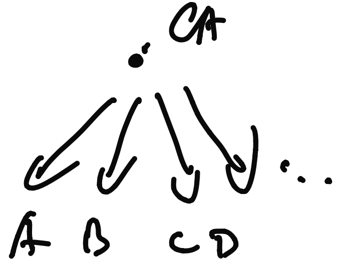
$$\text{cert}_{CA_1} = \text{sig}_{sk_{root}}(CA || pk_{CA_1})$$

$$\text{cert}_{CA_2} = \text{sig}_{sk_{CA_1}}(CA_2 || pk_{CA_2})$$

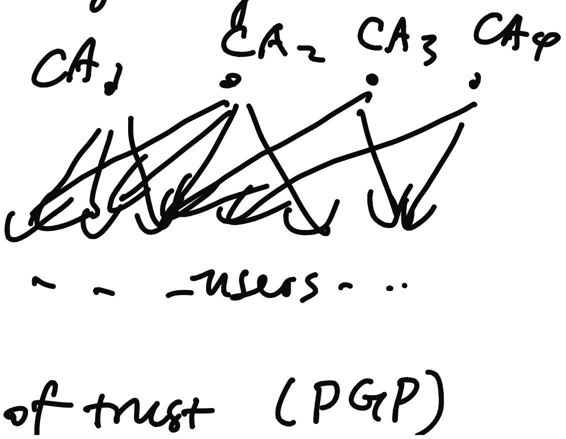
$$\text{cert}_{user_A} = \text{sig}_{sk_{CA_2}}(user_A || pk_{user_A})$$

chain of trust

Monopoly

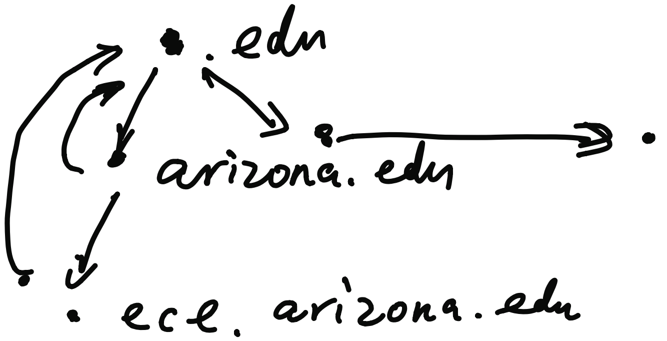


Oligarchy



Anarchy. // web of trust (PGP)

top-down with name constraints



pre-configured with root's PK.