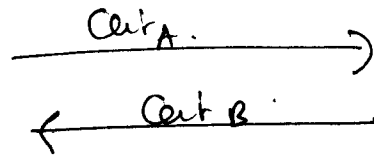


## Protocole DH avec certificats.

A

- Calculer  $k_{prA} \leftarrow a \cdot (alga)$   
 $A = \alpha^a \text{ mod } p$   
 $\text{Cert}_A = [(A, ID_A), A_A]$



- Vérifier certificat  
 $\text{Ver}_{k_{pub,CA}}(\text{Cert}_B)$
- Calculer la clé de session  
 $k_{AB} = B^a \text{ mod } p$

B

- Calculer  $k_{prB} \leftarrow b \cdot (alga)$   
 $B = \alpha^b \text{ mod } p$   
 $\text{Cert}_B = [(B, ID_B), A_B]$

- Vérifier certificat  
 $\text{Ver}_{k_{pub,CA}}(\text{Cert}_A)$
- Calculer clé de session  
 $k_{AB} = A^b \text{ mod } p$

## §5.3.2. PKI et CA.

- PKI = Public-Key Infrastructure est l'ensemble des techniques pour établir un système cryptographique à clé publique y compris la certification, qui est une tâche lourde à mettre en œuvre.
- La structure d'un certificat contient les informations techniques et personnelles : # série, algo de signature, autorité de certifi, période de validité, ID,  $k_{pub}$  et paramètres, etc.