Protocole DH avec certificats.

A	B
• Calculer $k_{prA} = a$ (aléa)	• Calculer $k_{prB} = b$ (aléa)
$A = \alpha^a \bmod p$.	$B = \alpha^b \bmod p$.
$Cert_A = [(A, ID_A), A_A]$.	$Cert_B = [(B, ID_B), A_B]$
$\xrightarrow{Cert_A}$	
$\xleftarrow{Cert_B}$	
• vérifier certificat $Ver_{k_{pub,CA}}(Cert_B)$.	• vérifier certificat $Ver_{k_{pub,CA}}(Cert_A)$
• Calculer la clé de session $k_{AB} = B^a \bmod p$.	• Calculer clé session $k_{AB} = A^b \bmod p$.

§§.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.