## A génère des clés et demande un certificat

A

A.

générer $k_{pubA}$, $k_{prA}$. $\xrightarrow{RQST(k_{pubA}, ID_A)}$

- vérifier $ID_A$
- $S_A = Sig_{prCA}(k_{pubA}, ID_A)$
- $Cert_A = [(k_{pubA}, ID_A), S_A]$.

$\xleftarrow{Cert_A}$

## CA génère les clés et les certificats.

A

CA

$\xrightarrow{RQST(ID_A)}$

- vérifier $ID_A$
- générer $k_{prA}, k_{pubA}$
- $S_A = Sig_{prCA}(k_{pubA}, IDA)$
- $Cert_A = [(k_{pubA}, IDA), S_A]$.

$\xleftarrow{(Cert_A, k_{prA})}$

Rq. Noter que, quand même, ce protocole est fait une seule fois (SET UP) par des canaux sûrs. Sinon pb!