# Établissement de clé

Shoutout to: https://letsencrypt.org/

## Certification signée par une autorité de confiance

- L'appareil du client vient pré-installé avec un "magasin de confiance" (trust store) contenant:
  - Nom de l'autorité de confiance
  - Clé publique de l'autorité de confiance
- Le serveur possède un certificat préalablement signé par l'autorité de confiance contenant:
  - Nom du serveur
  - Nom de l'autorité de confiance
  - Clé publique du serveur

# Établissement de clé

## Certification signée par une autorité de confiance

- Lors de l'établissement de clé, le serveur envoie au client:
  - $B$ la partie publique de sa clé de session Diffie-Hellman
  - Une signature $S_B$ de $B$ avec sa clé privée $K_{priv}$ fixe
  - La clé publique $K_{pub}$ correspondante pour vérifier la signature $S_B$
  - Une signature $S_{K_{pub}}$ de la clé publique émise par l'autorité de confiance
    - Vérifiable par le client avec la clé publique correspondante dans son trust store