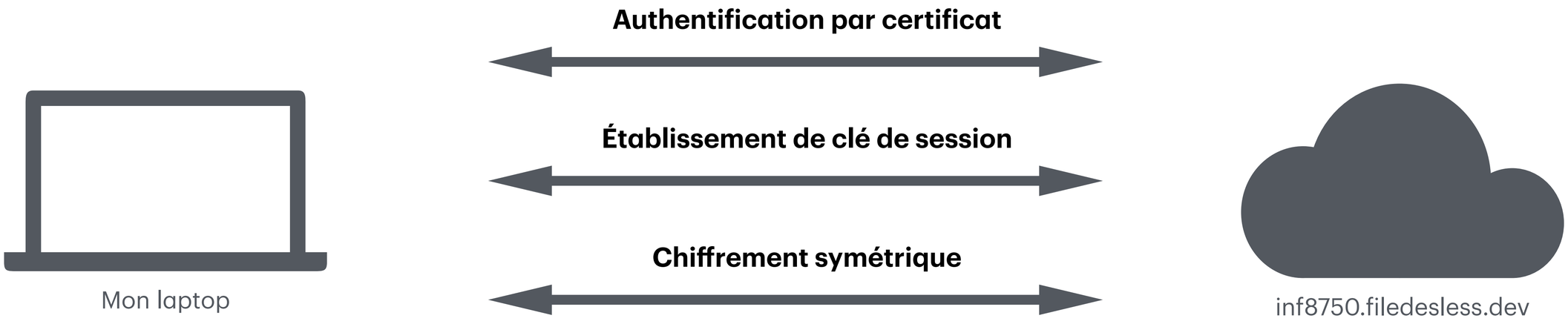
Introduction

Objectifs du labo

- Protocole TLS: Établissement de clé et certification
- Diffie-Hellman pour l'établissement de clé
  - Attaque de l'homme du milieu
  - Corps finis
  - Courbes elliptiques
- Certification et autorité de confiance

Connexion sécurisée HTTPS

Protocole Transport Layer Security (TLS)



En détails: https://tls13.xargs.org/