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

Établissement de clé

Algorithme de Diffie-Hellman sur les corps finis

g: générateur fixé d'un groupe cyclique

Hypothèse de sécurité: logarithme discret

Mon laptop

$a \in \mathbb{Z}_n$

$$A = g^a \mod p$$

$$B = g^b \mod p$$

inf8750.filedesless.dev

$b \in \mathbb{Z}_n$

Ex: ffdhe2048

From RFC 7919

g = 2

```
p = 2^2048 - 2^1984 + {[2^1918 * e] + 560316 } * 2^64 - 1
  = FFFFFFFF FFFFFFFF ADF85458 A2BB4A9A AFDC5620 273D3CF1
    D8B9C583 CE2D3695 A9E13641 146433FB CC939DCE 249B3EF9
    7D2FE363 630C75D8 F681B202 AEC4617A D3DF1ED5 D5FD6561
    2433F51F 5F066ED0 85636555 3DED1AF3 B557135E 7F57C935
    984F0C70 E0E68B77 E2A689DA F3EFE872 1DF158A1 36ADE735
    30ACCA4F 483A797A BC0AB182 B324FB61 D108A94B B2C8E3FB
    B96ADAB7 60D7F468 1D4F42A3 DE394DF4 AE56EDE7 6372BB19
    0B07A7C8 EE0A6D70 9E02FCE1 CDF7E2EC C03404CD 28342F61
    9172FE9C E98583FF 8E4F1232 EEF28183 C3FE3B1B 4C6FAD73
    3BB5FCBC 2EC22005 C58EF183 7D1683B2 C6F34A26 C1B2EFFA
    886B4238 61285C97 FFFFFFFF FFFFFFFF
```

$$s = B^a = g^{ab} \mod p$$

$$= A^b = g^{ab} \mod p$$