

Cachet

Développé par Colin Stefani & Simão Romano Schindler

Dans le cadre de l'unité « Développement d'applications internet »

<https://github.com/SchindlerSimao/cachet>

Table des matières

- Choix du projet,
- Fonctionnalités,
- Structure du projet,
- Détails d'implémentation,
- Suite / idées d'améliorations,
- Démo et questions.

Fonctionnalités



Génération de
clés Ed25519



Signature de
fichiers



Validation de
signature

Structure du projet

```

  ▾ src
    ▾ main
      ▾ java
        ▾ ch.heigvd
          ▾ commands
            © Cachet
            © Keygen
            © Sign
            © Verify
          > exceptions
          ▾ utils
            © FileIOUtils
            © KeyUtils
            © SignatureUtils
            © Constants
            © Main
        > test

```

Détails d'implémentation

- Courbe elliptique ED25519,
- Clé privée PKCS#8,
- Clé publique SPKI,
- Signature Base64,
- java.security pour éviter les dépendances externes.



Suite / idées d'améliorations

- Signer des répertoires de fichiers,
- Capacité de keygen à dériver une clé publique.