HTTPS chez Shopify

Maxime Boisvert

Moi

Production Engineer chez Shopify (Elasticsearch, k8s, HTTPS)

Maîtrise en TI (UQAM/Teluq) : Graphes de documents en recherche d'information juridique.

- Dirigé par Daniel Lemire (http://lemire.me/)
  - Roaring bitmaps (bitset compressé)
    - Apache Lucene
    - Elasticsearch
    - Google, Facebook, Shopify!

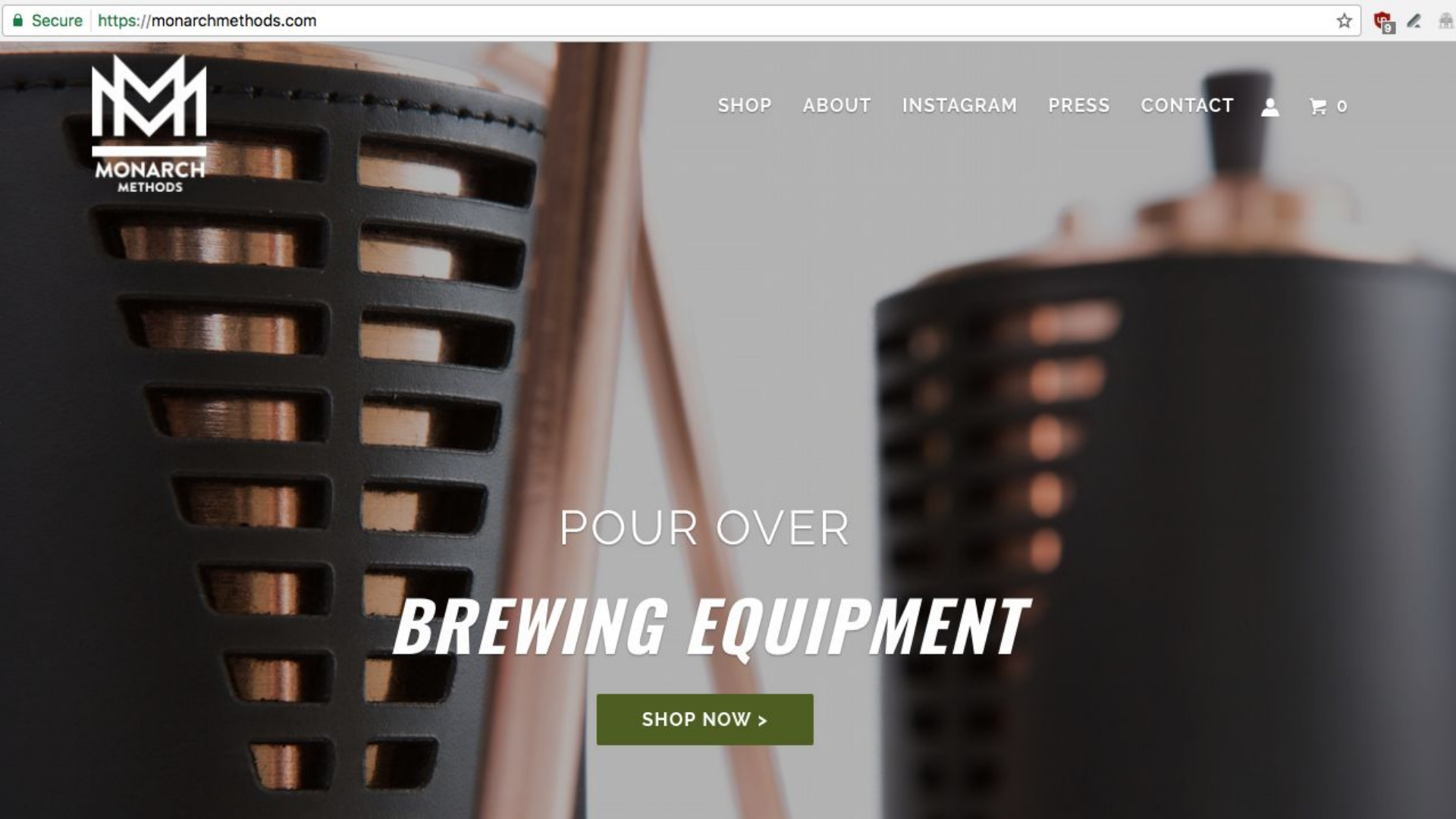
Shopify

- Plate-forme de commerce électronique pour créer des magasins en ligne
- Fondé en 2004
- Initialement un magasin de planches à neige (Snowdevil)
- +375000 entrepreneurs
- +29 milliards de dollars de vente

Exemple de clients : Foo Fighters, General Electric, Tesla Motors, Amnesty International, CrossFit, Pixar, Lollapalooza, Evernote, GitHub...

Vous?


Pourquoi HTTPS?
shopify


Secure
https://monarchmethods.com
MONARCH
METHODS
SHOP
ABOUT
INSTAGRAM
PRESS
CONTACT
0
POUR OVER
BREWING EQUIPMENT
SHOP NOW >

Cas d’utilisation

- Shopify application
  - https://MARCHAND_1.com
  - https://MARCHAND_2.com
  - https://MARCHAND_3.com
  - https://MARCHAND_4.com
  - https://MARCHAND_5.com
  - https://MARCHAND_6.com
  - ...

Google et HTTPS

- Meilleur SEO
  - Google I/O 2014 - HTTPS Everywhere announcement
    - Google utilise HTTPS pour ses services
  - HTTPS est un paramètre de l'algorithme de classement (août 2014)
    - Encouragé pour la sécurité des utilisateurs du Web
- Restriction de HTTP sur Chrome en 2017
  - Announcé en septembre 2016
  - Étiquette "Not secure" pour les pages HTTP avec
    - <input type=password>
    - Formulaire de paiement par carte de crédit détecté
  - Sera affiché pour toutes les pages HTTP dans le future

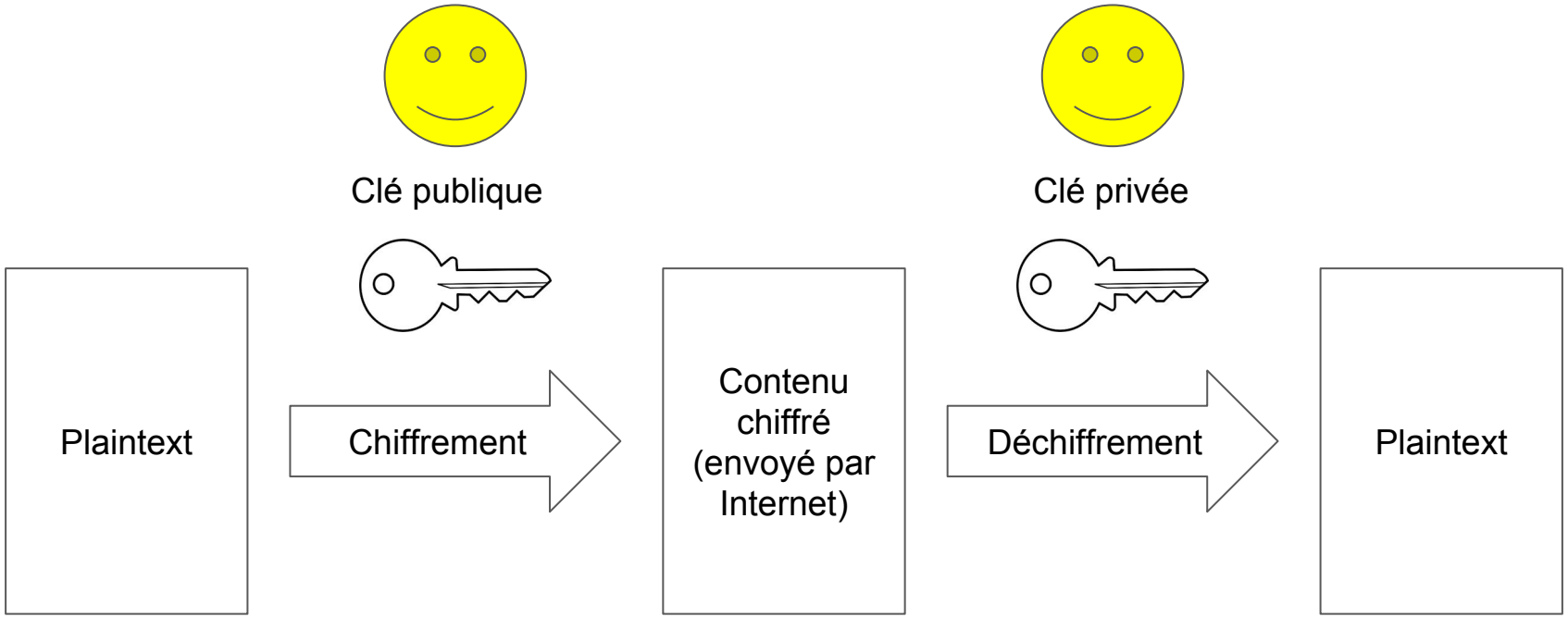
Protection des données des usagers

(La vrai raison)

- Données reçues authentique
  - E.g. Publicités ajoutées par un accès Internet non-sécurisé
- Données transmise illisibles par un intermédiaire


Sécurité et Web
shopify

Infrastructure à clés publiques (PKI)



Certificat

- Autorité (CA)
- Identité
- Clé publique

HTTPS

- Couche de communication sécurisée par dessus HTTP
- HTTP + Sécurité/SSL

SSL / TLS

- Protocols de chiffrement
- Utilisé pour authentification et chiffrement
- SSL (Secure Sockets Layer)
  - SSL 2.0 1995
  - SSL 3.0 1996
  - Obsolète depuis juin 2015
- TLS (Transport Layer Security)
  - TLS 1.0 1999 (basé sur SSL 3.0)
  - Vieux navigateur pas toujours supportés
  - Encore appelé SSL

SAN / SNI

- SAN (Subject Alternative Name)
  - Un certificat pour plusieurs noms de domaine
  - Utilisé pour les EV certificats de secours chez Shopify
- SNI (Server Name Indication)
  - Une adresse IP
  - Plusieurs noms de domaine
  - Un certificat par nom de domaine
  - Utilise TLS
  - Nom de domaine spécifié au moment de la connection
- Non TLS browser
  - Pas supporté chez Shopify


Obtenir des certificats
shopify

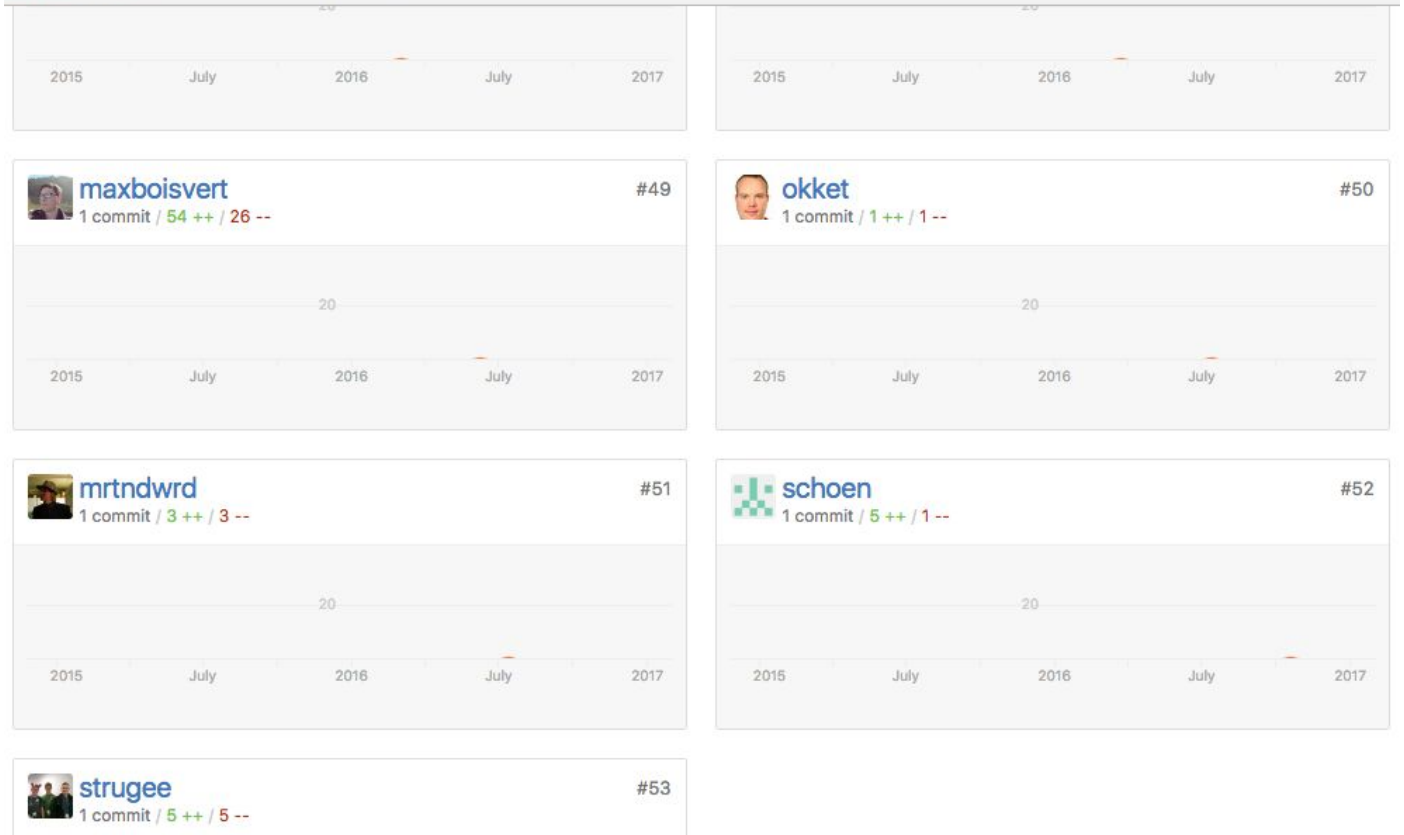
Let’s Encrypt

- Autorité de certification (CA)
- Gratuit
- Processus qui s’automatise

MAJOR SPONSORS

Open source

https://github.com/letsencrypt/boulder/graphs/contributors



Let’s Encrypt

ACME (Automatic Certificate Management Environment)

- Protocol de l’API pour obtenir un certificat
  - Créer un compte
  - Soumettre une demande de certificat
  - Vérification de la propriété du nom de domaine du certificat
  - Attendre l'émission
  - télécharger le certificat

Let’s Encrypt

- Choisir un client selon le langage utilisé
  - https://letsencrypt.org/docs/client-options/
- Client ruby utilisé chez Shopify
  - https://github.com/unixcharles/acme-client
- Débuter avec certbot
  - https://certbot.eff.org/
  - Apache
  - Nginx


Shopify
shopify

Shopify

Problèmes

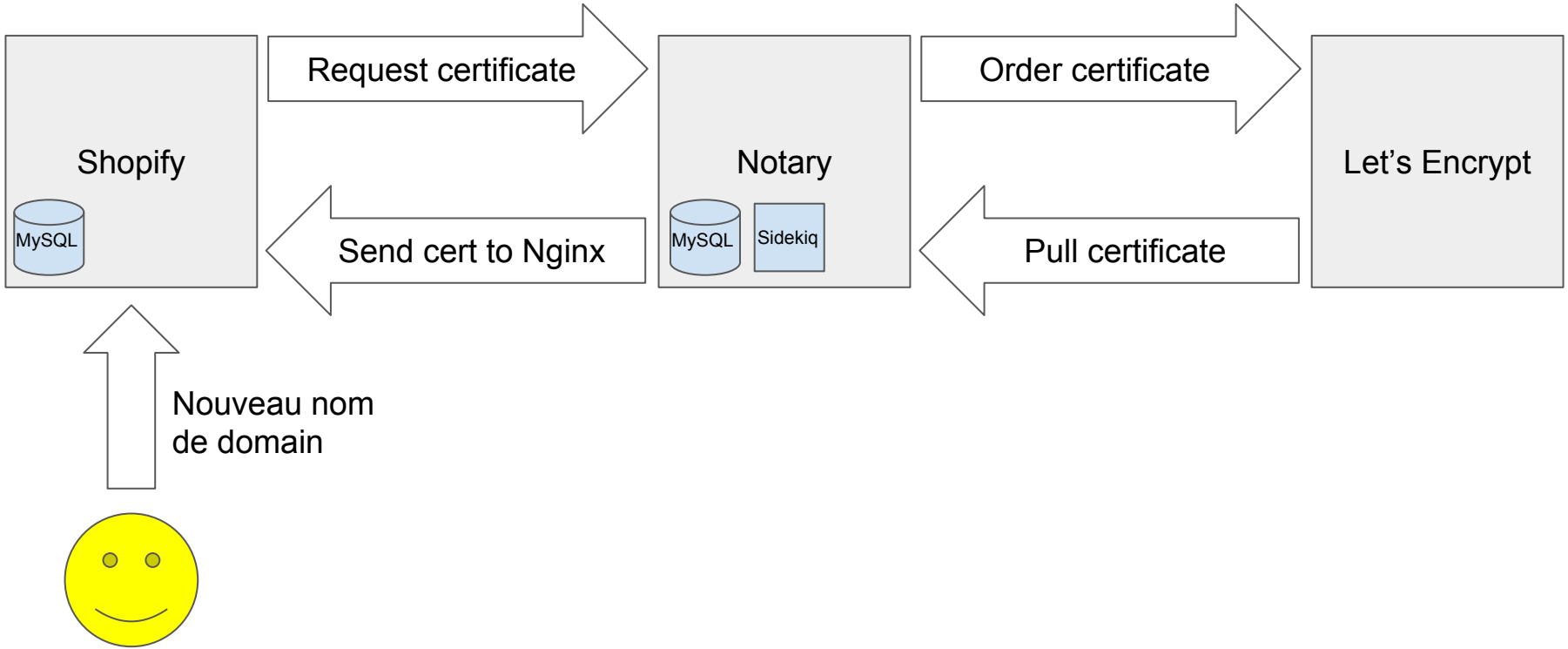
- Commander les certificats
- Renouveler les certificats
- À grande échelle

Architecture

- Ruby on Rails
  - Applications
    - Shopify
    - Notary (application dédiée pour gérer les certificats)
  - Base de données (MySQL)
  - API REST
- Sidekiq
  - Exécute les différentes tâches récurrente
  - Flot de données pour commander les certificats

Sidekiq

Architecture de Shopify



Questions?

- https://github.com/maxboisvert/HTTPS-WAQ17
- maxime.boisvert@shopify.com