Sigstore: rendre les signatures digitales accessibles à tous

OSSIR - 14 Novembre 2023

Maya Costantini
Software Engineer, Red Hat

$whoami

- Software Engineer, Red Hat Emerging Tech Security team 
- Contributrice Open Source
- Sécurité de la chaîne d’approvisionnement logicielle
- Dev Python

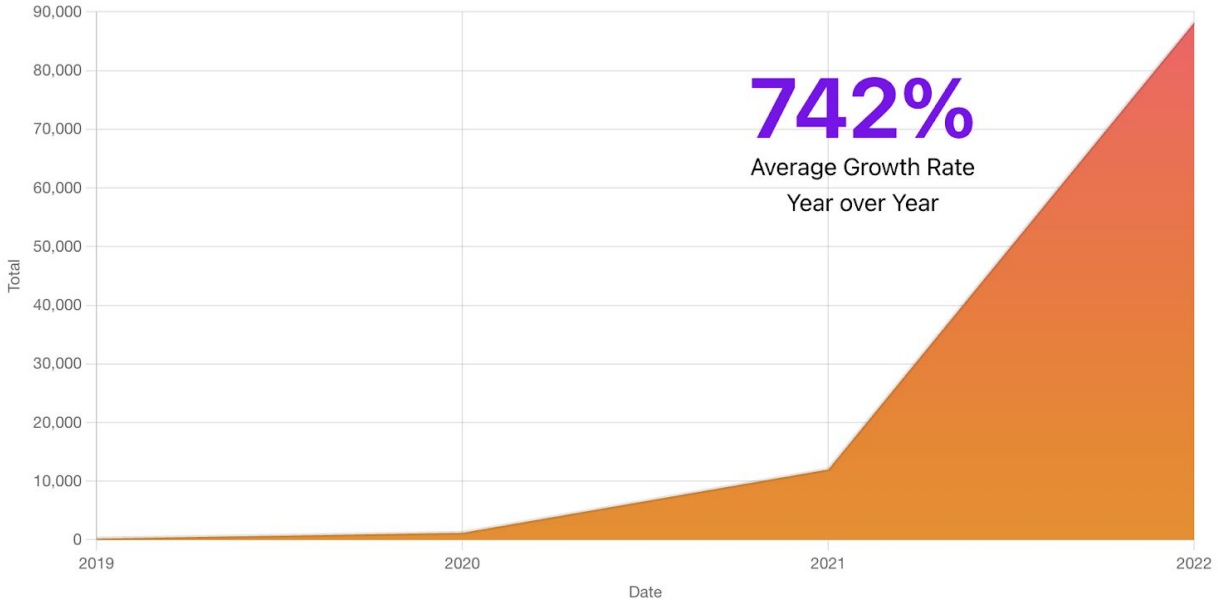
@mayacostantini@hachyderm.io

@MayaCostantini

@mayaCostantini

Sécurité de la chaîne d’approvisionnement: pourquoi en parle-t-on autant?

FIGURE 1.6. NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS, 2019–2022



Source: *https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-demand-security*

Sécurité de la chaîne d’approvisionnement: pourquoi en parle-t-on autant?

Face à cette menace:

- De nouvelles régulations:
  - US Executive Order 14028 on Improving the Nation’s Cybersecurity
  - European Union Cyber Resilience Act
- Des standards émergeants au sein des communautés Open Source:
  - The Update Framework (TUF)
  - in-toto
  - SLSA
  - **Sigstore**

Le rôle des signatures digitales dans la sécurité de la chaîne d’approvisionnement

- Les attaquants jouent sur les attentes de **reproductibilité** des développeurs pour trouver des maillons faibles dans une chaîne d'approvisionnement logicielle
- Les signatures cryptographiques garantissent:
  - **Authenticité**
  - **Intégrité**

Les signatures cryptographiques: avant Sigstore

Défis posés par OpenPGP/GPG:

- Veiller à ce que les bonnes clés publiques arrivent à leurs destinataires
- Stockage des clés privées
- Rotation régulière des clés privées pour éviter les compromis
- Options de ligne de commande complexes
- Besoin occasionnel de connaissances en cryptographie

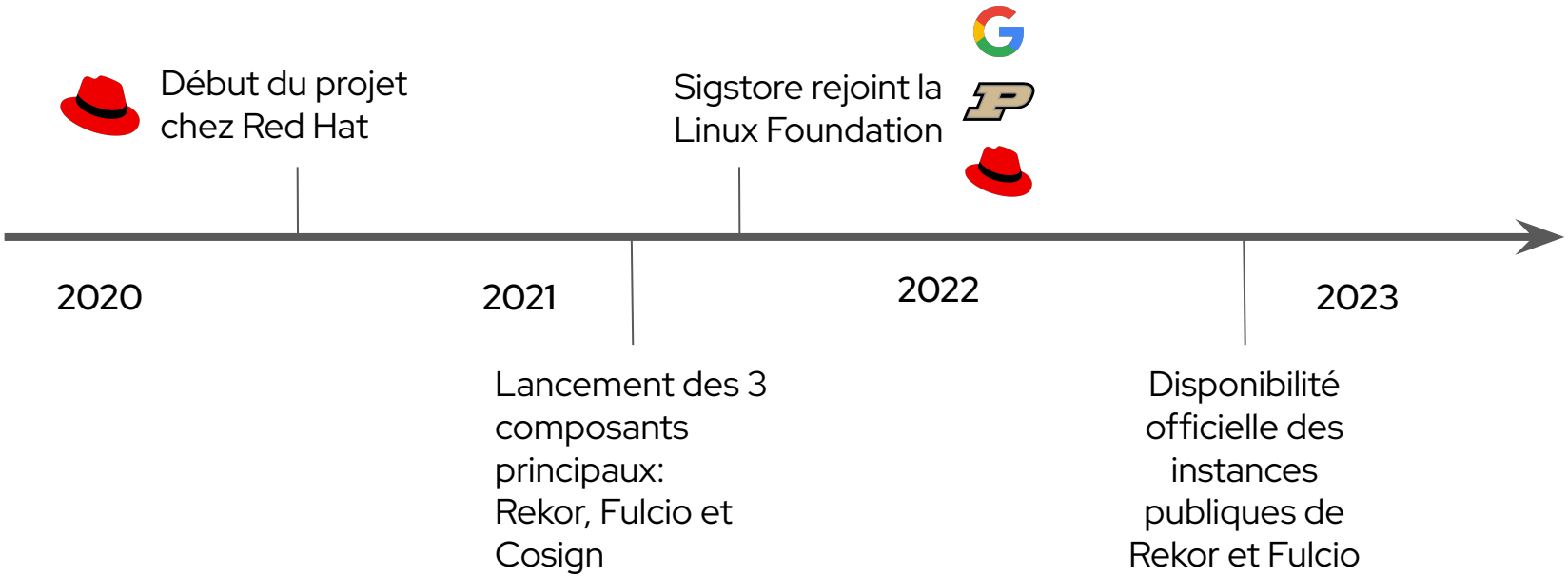
Une “key signing party”, FOSDEM 2008, [Wikipedia]

“Devenir aux signatures cryptographiques ce que Let’s Encrypt est à HTTPS”

- Une autorité de certification gratuite et automatisée
- Tout propriétaire de domaine peut obtenir un certificat gratuitement
- Plus de 290M de certificats délivrés depuis 2016

- Un service gratuit pour signer des artéfacts numériques
- Les signatures sont enregistrées dans un registre transparent et public
- Plus de 48 millions d'entrées stockées depuis 2021

Historique


Début du projet chez Red Hat
Sigstore rejoint la Linux Foundation
2020
2021
2022
2023
Lancement des 3 composants principaux: Rekor, Fulcio et Cosign
Disponibilité officielle des instances publiques de Rekor et Fulcio

Pourquoi Sigstore?

Pour résoudre les principaux problèmes posés par OpenPGP:

- Pas de connaissance en cryptographie ou des protocoles PKI n'est requise.
- Une interface simple pour rendre les signatures digitales accessible à tous
- Plus de gestion et de rotation des clés privées
- Audit et révocation plus faciles en cas de compromission.
- Les signatures sont liées à une **identité publique** plutôt qu'à une clé publique grâce au protocole OpenID Connect (**“keyless signing”**)

Faire adopter les signatures digitales au plus grand nombre des développeurs

Les composants de Sigstore

Transparency Log

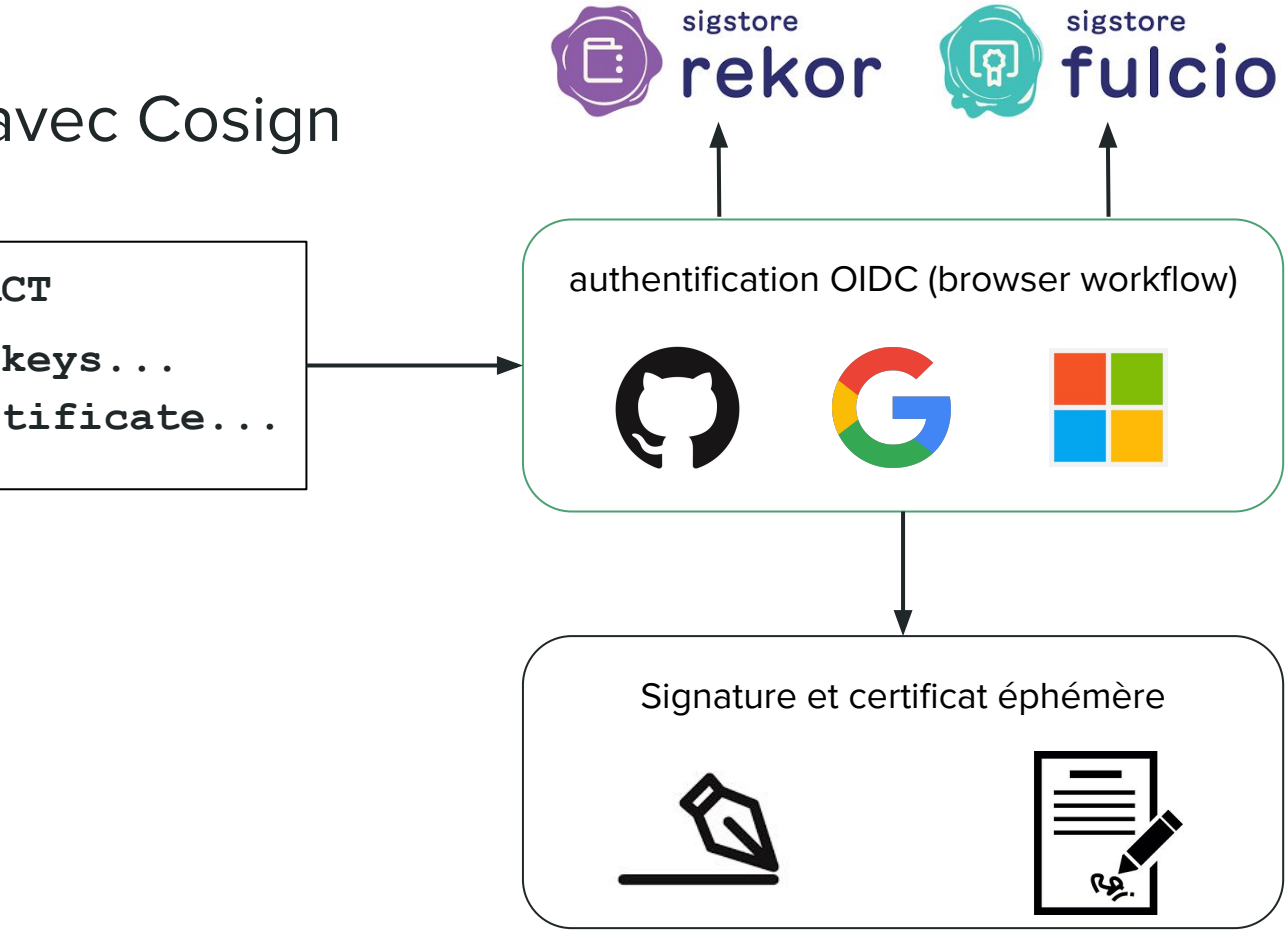
Autorité de certification gratuite

Client (Golang) pour signer et vérifier des artéfacts

+ Autres clients (Python, JavaScript, Rust...)

Signer un artifact avec Cosign

```
$ cosign sign $ARTIFACT
Generating ephemeral keys...
Retrieving signed certificate...
```



Vérifier un artifact avec Cosign

```
$ cosign verify \
--cert cert.pem \
--certificate-oidc-issuer https://oauth.github.com \
--certificate-identity user@example.com \
$IMAGE
```

Rejoignez la communauté Sigstore

sigstore.dev/community

https://links.sigstore.dev/slack-invite

Sigstore YouTube channel

sigstore Blog https://blog.sigstore.dev/