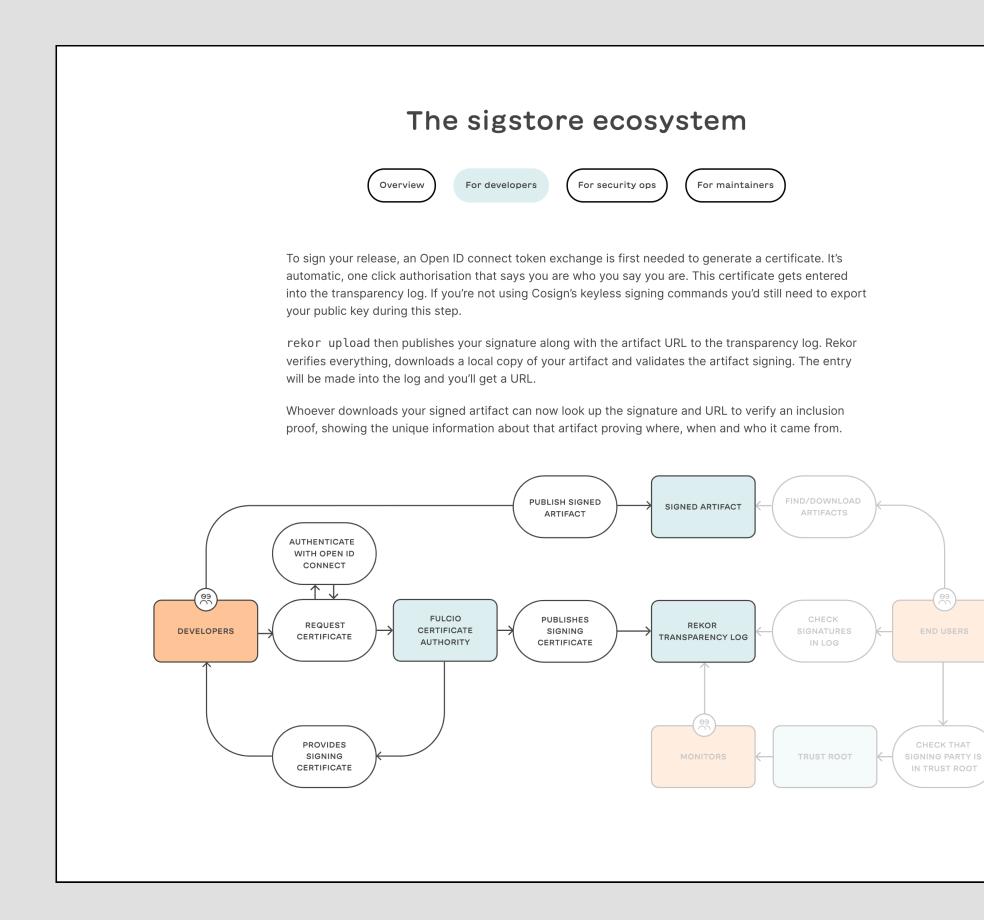READY FOR DEV

sigstore
How sigstore works

A new standard for signing, verifying and protecting software

Making sure your software's what it claims to be.

In collaboration with

Google   THE LINUX FOUNDATION   Red Hat   PURDUE UNIVERSITY

The sigstore ecosystem

To sign your release, an Open ID connect token exchange is first needed to generate a certificate. It's automatic, one click authorisation that says you are who you say you are. This certificate gets entered into the transparency log. If you're not using Cosign's keyless signing commands you'd still need to export your public key during this step.

rekor upload then publishes your signature along with the artifact URL to the transparency log. Rekor verifies everything, downloads a local copy of your artifact and validates the artifact signing. The entry will be made into the log and you'll get a URL.

Whoever downloads your signed artifact can now look up the signature and URL to verify an inclusion proof, showing the unique information about that artifact proving where, when and who it came from.

sigstore

Content designer (freelance)
www.sigstore.dev
2021

Work with Projects by IF has been on their contracts with the OpenSSF, which include clients from Google, Red Hat, the Linux Foundation and Purdue, designing new websites for their projects in the open source security space.

http://sigstore.dev is the finished, public site for sigstore, a non-profit collective working to make software signing easier. It's main aims were to increase adoption and make it easier for a wider audience to understand just what's going on, and the new urgency around the topic (2021's Executive Orders shot cybersecurity up the priorities).

There wasn't a lot to go on, and any existing content lived in GitHub repos and several recordings by developers for developers. We needed to include policymakers, general public, security experts, and the international developer community. The content works especially hard to provide a clear picture of how the tech works, the central value propositions and a stamp of authority.

I'd run the developing content by the working group, synthesising the complication technicalities into content a little more easier to parse.

The handover, rollout, and subsequent success of the program all went smoothly. There's now over 1,200 members of the group, over 2,800+ commits, and significant governmental-level attention to help more people learn and start using the solution.