Linux Foundation Announces Free sigstore Signing Service to Confirm Origin and Authenticity of Software

Red Hat, Google and Purdue University lead efforts to ensure software maintainers, distributors and consumers have full confidence in their code, artifacts and tooling

SAN FRANCISCO, Calif., March 9, 2021 – The Linux Foundation, the nonprofit organization enabling mass innovation through open source, today announced the sigstore project. sigstore improves the security of the software supply chain by enabling the easy adoption of cryptographic software signing backed by transparency log technologies.

sigstore will empower software developers to securely sign software artifacts such as release files, container images and binaries. Signing materials are then stored in a tamper-proof public log. The service will be free to use for all developers and software providers, with the sigstore code and operation tooling developed by the sigstore community. Founding members include Red Hat, Google and Purdue University.

"sigstore enables all open source communities to sign their software and combines provenance, integrity and discoverability to create a transparent and auditable software supply chain," said Luke Hinds, Security Engineering Lead, Red Hat office of the CTO. "By hosting this collaboration at the Linux Foundation, we can accelerate our work in sigstore and support the ongoing adoption and impact of open source software and development."

Understanding and confirming the origin and authenticity of software relies on an often disparate set of approaches and

data formats. The solutions that do exist, often rely on digests that are stored on insecure systems that are susceptible to tampering and can lead to various attacks such as swapping out of digests or users falling prey to targeted attacks.

“Securing a software deployment ought to start with making sure we’re running the software we think we are. Sigstore represents a great opportunity to bring more confidence and transparency to the open source software supply chain,” said Josh Aas, executive director, ISRG | Let’s Encrypt.

Very few open source projects cryptographically sign software release artifacts. This is largely due to the challenges software maintainers face on key management, key compromise / revocation and the distribution of public keys and artifact digests. In turn, users are left to seek out which keys to trust and learn steps needed to validate signing. Further problems exist in how digests and public keys are distributed, often stored on websites susceptible to hacks or a README file situated on a public git repository. sigstore seeks to solve these issues by utilization of short lived ephemeral keys with a trust root leveraged from an open and auditable public transparency logs.

“I am very excited about the prospects of a system like sigstore. The software ecosystem is in dire need of something like it to report the state of the supply chain. I envision that, with sigstore answering all the questions about software sources and ownership, we can start asking the questions regarding software destinations, consumers, compliance (legal and otherwise), to identify criminal networks and secure critical software infrastructure. This will set a new tone in the software supply chain security conversation,” said Santiago Torres-Arias, Assistant Professor of Electrical and Computer Engineering, University of Purdue / in-toto project founder.

“sigstore is poised to advance the state of the art in open source development,” said Mike Dolan, senior vice president and general manager of Projects at the Linux Foundation. “We are happy to host and contribute to work that enables software maintainers and consumers alike to more easily manage their open source software and security.”

“sigstore aims to make all releases of open source software verifiable, and easy for users to actually verify them. I’m hoping we can make this easy as exiting vim,” Dan Lorenc, Google Open Source Security Team. “Watching this take shape in the open has been fun. It’s great to see sigstore in a stable home.”

For more information and to contribute, please visit: https://sigstore.dev

About the Linux Foundation

Founded in 2000, the Linux Foundation is supported by more than 1,000 members and is the world’s leading home for collaboration on open source software, open standards, open data, and open hardware. Linux Foundation’s projects are critical to the world’s infrastructure including Linux, Kubernetes, Node.js, and more. The Linux Foundation’s methodology focuses on leveraging best practices and addressing the needs of contributors, users and solution providers to create sustainable models for open collaboration. For more information, please visit us at linuxfoundation.org.

###

Media Contact

Jennifer Cloer

for Linux Foundation

503-867-2304

jennifer@storychangesculture.com

The post Linux Foundation Announces Free sigstore Signing Service to Confirm Origin and Authenticity of Software appeared first on Linux Foundation.