CodeLocker

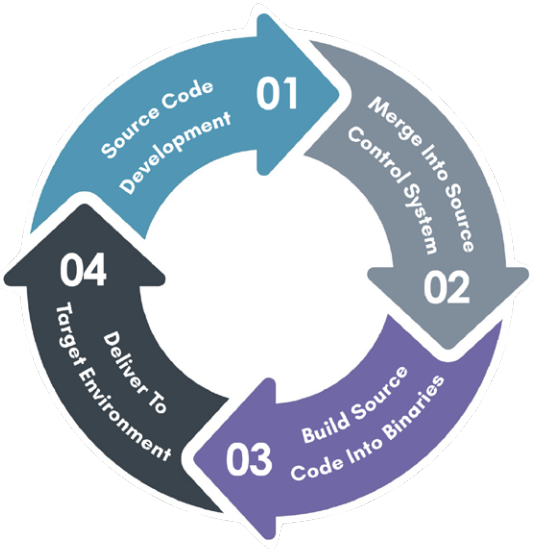
Achieve End-to-End Software Governance Using Zeva's CodeLocker

Software provenance needs to start with the developer and at the code level. CodeLocker, integrated within the SDLC DevOps, uses non-repudiation and trusted digital signatures on source code, audit logs, and builds of software and containers. CodeLocker provides an automated way to sign source code commits and the build artifacts providing end-to-end software provenance and non-repudiation of software artifacts

Software supply-chain attacks have long been a serious threat, with malware infiltrating build pipelines and compromising software integrity without detection. These vulnerabilities can emerge at any stage of the development lifecycle, making strong security measures essential. Tools like CodeLocker help mitigate these risks by ensuring end-to-end software provenance through trusted digital signatures and audit logs.

Solution

CodeLocker addresses many of the recommended secure software development framework practices outlined in NIST 800-218. CodeLocker starts with signing the developer's source code, signing during the review, approval, and commit process, and finishes with signing the build/ container for deployment. It uses a centralized private key operation so that clients do not possess private keys. Instead, the private key is stored in an HSM, processed by CodeLocker, and source code always stays at the client. This process makes key management easier, while increasing security. In addition, CodeLocker implements Long Term Validation (LTV) signatures specifically for air-gapped target environments so that the signature never expires and can contain all the data necessary to validate within those sequestered environments.



Benefits

Focusing on the full development lifecycle makes CodeLocker a market **differentiator**. Our solution integrates with existing software development processes, identity management tools, git, DevOps, and source control platforms. Even if the environment is connected and sequestered, you can maintain control of your centralized organizational private key. CodeLocker easily integrates with your existing environment and provides a cost-effective way to maintain software provenance.

Software Development Supply Chain

- Code/Organizational level certificate signing
- Eliminates the need for developers to provide their code signing private keys to third party systems
- Multiple authentication and verification with step-by-step audit

Integration with Other Development Tools

- Integration with many repository solutions to sign code commits
- Integration with built servers (CI/CD) to sign built outputs thus increasing efficiency
- Customizable plug-ins to extend third-party applications

Centralized Private Key Control

- Keys stay protected at FIPS 140-2 L3
- Complies with Federal PKI regulations and retains control within the agency
- Takes advantage of existing investment in PKI and CA infrastructure with S/MIME certificates

ROI Advantages

- Easy to implement, easily integrates with existing git repos, and dev/ops build software
- Cost-effective when compared to individual developer signing and Authenticode tokens
- Reduces administrative burdens and increases efficiencies by automating key signing and key management process

Expanded File Signing Support

- Includes support for Container Image signing
- Includes support for signing: All ELF extension files, .java, .python, .properties, .iss, .bat, .h, .cpp, .py, .go, .yaml, .json

Linux Signature Validation Service

- Ensures code integrity before execution
- Ability to verify the Container Image signature before running

zeva

Over two decades of Public Key Enablement (PKE), Identity, Credentialing, and Access Management (ICAM) excellence. Throughout the years, Zeva has been solving the most complex identity and encryption challenges for the federal government and corporations around the globe.

Zeva Incorporated, a Zeva Holdings company, helps clients around the globe strengthen their security posture with tailored services. Founded in 2005, in Herndon, Virginia, USA; Zeva Inc. is a CMMI Level 3, Woman-Owned Small Business. Zeva develops and licenses commercial off-the-shelf (COTS) products that address the PKI enablement needs of highly regulated agencies. Demonstrating its market dominance, Zeva holds multiple patents for encryption and decryption technologies.

Sample of Zeva's Customers

IRS, UBS, Deutsche Bank, Chevron, Northrop Grumman, bp, Sandia National Laboratories, Glencore

ISO 9001 · SBA WOSB Woman Owned Small Business · certified WBENC Women's Business Enterprise

ISO 20000 · ISO 27001 · CMMI DEV/3 · CMMI SVC/3

MAS Contract:
GS-35F-0476X

GSA Contract Holder

NASA SEWP V

DUNS Number:
828301577

CAGE Code:
60JZ1

10300 Eaton Place
Suite 305,
Fairfax, VA 22030

info@zevainc.com
(888) 938-2462
www.zevainc.com