DigiCert® KeyLocker

Cloud-based code signing key management for small software teams

Secure your private code signing keys to ensure software authenticity, integrity, and compliance.

Overview

Don't wait for your token to get lost in shipping or in someone's desk drawer. DigiCert KeyLocker provides cloud-based secure key storage, key generation, and signing without the constraints of a physical token.

It is best for individual developers and small teams who sign code occasionally. KeyLocker can be purchased with a code signing certificate via CertCentral, making key protection that meets CA/B Forum requirements easy to obtain, set up, and use.

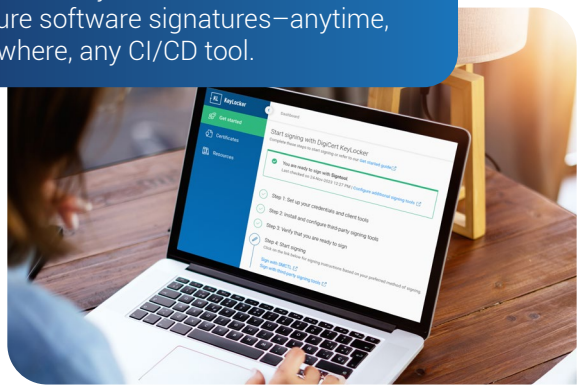
Compliant & Convenient

- **Strong, compliant storage:** Meet CA/B Forum requirements for secure key storage without the expense of on-premises HSMs or the constraints of physical tokens.
- **Sign from anywhere:** Cloud-based storage facilitates secure code signing for remote developers.
- **Easy to buy:** Get KeyLocker in CertCentral with your code signing certificate and eliminate the wait for token shipment.
- **Easy to use:** Automatic generation of CSRs and private keys. Auto-renewed certificates preserve their association with keys.
- **Integrate seamlessly:** Set your keypair alias and automate pipeline workflows through integrations with modern CI/CD platforms.

KeyLocker Secured Certificate Details

- Certificate with RSA 3072 keypair
- Includes up to 1,000 code signings per certificate per year. (Purchase additional units to enable more signings.)
- 1-, 2-, and 3-year certificates available.
- Keypair stored on FIPS 140-2 Level 3 cloud-based HSM.
- One active signer per certificate. Signer can be changed at any time by the KeyLocker Lead.
- Batch signing functionality via CLI.

DigiCert® KeyLocker enables automated secure software signatures—anytime, anywhere, any CI/CD tool.



NEED MORE? For organizations that have global software teams, multiple development and release tech stacks, or are regularly audited, explore DigiCert's Software Trust Manager.

Govern code signing and release trusted software with centralized visibility and enforcement, decentralized operations and use. Policy-driven controls include role-based access, irrefutable audit logs, threat detection, and SBOM management.