Code Signing Certificate Options Comparison

A code signing certificate is only the starting point to securing your software. Protecting the private key, renewing or revoking the certificate, signing consistently, and proving who signed what requires additional work.

Solutions like DigiCert® Software Trust Manager Essentials and Advanced give you the physical security of an HSM and the ease of cloud storage in addition to certificate management, advanced code signing tools, and CI/CD integrations that certificates alone don't include. Also, gain release risk visibility through monitoring of your GitHub repositories.

Function	USB Token	Your HSM[2]	DigiCert KeyLocker[3]	Software Trust Manager Essentials	Software Trust Manager Advanced
Key protection & everyday signing					
Compliant[1] code signing key storage	Yes	Yes	Yes	Yes	Yes
Managed, secure, cloud-based storage service	No	No	Yes	Yes	Yes
Secure signing from anywhere	No	You build	Yes	Yes	Yes
Integration with CI/CD platforms	No	You build	Yes	Yes	Yes
Automation with CLI and API	No	You build	Yes	Yes	Yes
Certificate management					
Certificate management in one console (issue, track, renew)	Manual	Manual	Manual	Yes	Yes
Manage public and private trust keypairs	Public Only	You build	Public only	Public only	Yes
Auto-renew capable	No	No	Yes	Yes	Yes
Signers per keypair	You build	You build	1	1	Up to 10
Governance & release security					
Visibility into release vulnerabilities	No	No	No	Yes	Yes
Continuous monitoring of release vulnerabilities	No	No	No	No	Yes
Email and GitHub alert notifications	No	No	No	Yes	Yes
Audit-ready signature and activity logs	No	No	No	No	Yes
Single sign-on (SSO)	No	No	No	No	Yes
Test and manifest signing; algorithms beyond RSA	No	No	No	No	Yes

1. Compliant with FIPS 140-2 Level 3 or CC EAL 4+ as required by CA/Browser Forum Baseline Requirements
2. "Your HSM" is a hardware security module you purchase, host, and operate yourself (on-premises or in your own cloud). "You build" means the capability depends on integrations you create and maintain.
3. Included for comparison of products you may have. KeyLocker is End of Sale and not available for new customers.

The hidden work behind a certificate

- **Key protection.** Private keys must live in FIPS 140-2 Level 3 or CC EAL 4+ compliant hardware. Tokens have to be shipped, stored with physical security, and replaced if lost. An HSM must be bought, hosted, connected, patched, and backed up.
- **Access.** Tokens need physical access control, and sharing them with a team or a CI/CD pipeline invites workarounds that weaken security.
- **Lifecycle.** Renewals, reissues, and key rotations are manual on token and your HSM, and an expired certificate can halt a release.
- **Proof.** Without signing logs, it's hard to show who signed what, when, and under which policy.
- **Risk.** A release that ships with a known vulnerability still carries your signature.

Choosing the right fit

USB Token — Best for an individual who signs occasionally from one machine. You manage a physical device, and there is no cloud, CI/CD, or audit capability needed.

Your HSM — Best for organizations that already run HSMs and have the staff to build and maintain signing integrations, access control, and audit trails. Note that higher capacity HSMs will be needed in the near future to accommodate PQC algorithms.[1]

KeyLocker — This product is end of sale and not available to new customers. Existing customers can renew their KeyLocker certificates. KeyLocker is expected to be retired in 2027.

Software Trust Manager Essentials — Best for developers and startups that want HSM-grade security with cloud convenience. Adds certificate management, CI/CD integrations including CLI and API support, and visibility into release vulnerabilities. **Starting at $83/month** (500 signatures, 12-month auto-renewing $1,000 subscription).

Software Trust Manager Advanced — Best for growing teams that need centralized control, multiple signers per key, public and private trust keypairs, SSO, audit logs, continuous vulnerability monitoring, test and manifest signing, or algorithms beyond RSA. Contact sales for pricing.

1. Post-quantum signatures and keys are much larger than RSA. A 2,048-bit RSA key produces a 256-byte signature and has a 256-byte public key; ML-DSA (FIPS 204) signatures are 2,420 to 4,627 bytes and public keys 1,312 to 2,592 bytes — roughly 9 to 18 times larger signatures.

Pricing shown is the starting price at the minimum 500 signatures and may change; confirm at digicert.com.

Need even more? Software Trust Manager Premium adds unlimited signers, container and Apple file signing, bulk and selective signing for high volume, hybrid cloud and on-premises HSM, and dedicated technical support.

Visit digicert.com/software-trust-manager

About DigiCert

DigiCert is a global leader in Intelligent Trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.

© 2026 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.