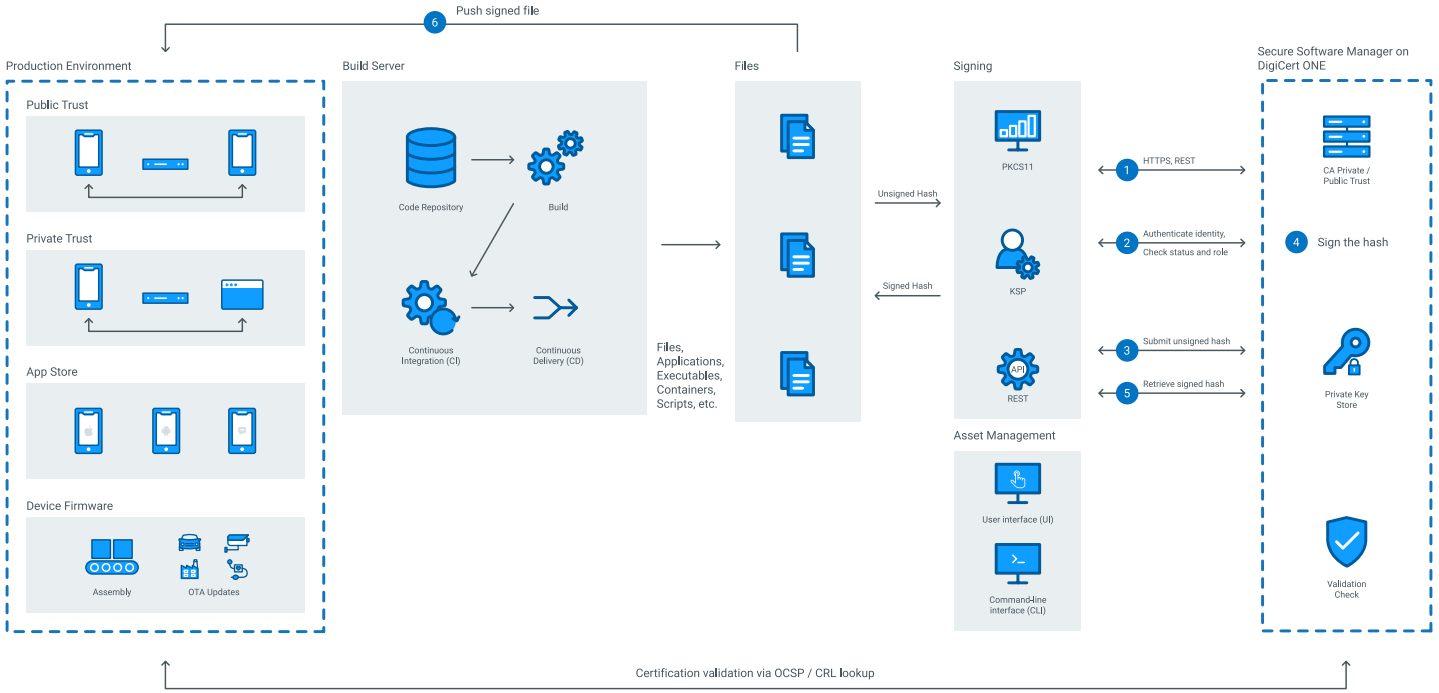
Continuous Integration/Continuous Delivery with DigiCert Secure Software Manager

Modern code signing for CI/CD processes

Software development teams used to build products first and test later. Over the years, they learned that guessing is gambling. But isn't agile development without security gambling, too? With DigiCert Secure Software Manager, DevOps can be agile and secure at the same time.

Secure Software Manager drives code signing expediency and efficiency

Code signing assures that your code has not been altered since it was signed. To ensure the integrity of the code, a PKI certificate provides encryption, authentication and identity before Quality Assurance tests and product delivery. The diagram below shows how Secure Software Manager makes it easy for DevOps teams to seamlessly incorporate secure and high-performance code signing with automation build tools in use.



digicert®

Automate code signing for agile development

- Leverage DigiCert client-side libraries (KSP and PKCS11) to support integration directly with CI/CD platforms for automation
- Use the Secure Software Manager hash signing approach to provide local signing speed for large files while maintaining key protection and signing event auditing records
- Make use of support for scripted integration of client-side libraries like Microsoft KSP, PKCS#11, and Apple KryptoTokenKit, as well as direct integration of CSP with major CI/CD platforms including Apache Maven, Gradie, Jenkins, and Azure DevOps
- Timestamping services can be included as part of the signing request

Enhanced code signing security

- Secure Software Manager maximizes security with multiple key signing models including single usage and on-demand keys. These key signing models are aligned with major signing platforms and with your needs.
- With permission-based controls, you can specify access and privileges for any individual in your organization for signing and administration. In the event of personnel changes, you can adjust access levels quickly and securely from a centralized control panel. A build server can be configured as an API user so that signing requests can be made without the need for human intervention.
- Easily export in-depth reports and logs track signed code and activity. For a more automated process, you can request reports and audits over APIs.
- Ensure code signing activities are only accessible from a specific IP range with restricted authentication by IP address

High performance for high-volume development

- Secure Software Manager expedites the secure signing of large files by performing “hash” signing, eliminating the need to transfer the actual source files of application to the cloud for signing
- Secure Software Manager supports hash signing in all files, including public Extended Validation (EV) and Organization Validation (OV) and private code signing, as well as for all major binary types, including Microsoft Authenticode, Java, Android, and Docker

For more information on Secure Software Manager, contact one of our PKI experts at pki_info@digicert.com