digicert®

Hash signing with DigiCert Secure Software Manager

Quickly and easily secure code with hash signing

In our connected world, businesses and users rely on file sharing for everything from software and app releases to patches and updates. But with many security solutions, signing code means giving up control over the very files you're trying to protect.

With DigiCert Secure Software Manager, files are never uploaded, so your valuable property stays at all times inside your environment. More, hash signing helps you avoid common local signing management issues like key protection and user access. It's the best of both worlds—the speed of local signing with the security assurance of the cloud.

How does hash signing work?

1. Client-side libraries, including KSP for Windows and PKCS11 for all others, facilitate a working partnership between Secure Software Manager APIs and the local signing tool
2. Client-side libraries enable the secure signing of large files by generating the hash of the requested application, then sending that hash to Secure Software manager, where it's signed in the cloud with a protected private key
3. When cloud signing is complete, the client-side libraries give the signed hash back to the signing tool, where the signature integrates with the original application. Now, the original application is signed, having never left your environment.

Key features and benefits

1. **Expedite**
   Signing a 1.95GB file with a 5MB/s connection takes approximately 24 seconds
2. **Protect**
   Unsigned software never leaves your organization's environment
3. **Control**
   Client-side libraries can be called in conjunction with local signing tools via command prompt
4. **Support**
   Full integration into CI/CD for signing automation using common tools like Azure DevOps, Jenkins, ANT, Gradle, and Apache Maven
5. **Manage**
   Fully integrated with Secure Software Manager APIs to support user access management, private key protection and auditing of all code signing events

Cloud signing without hash	Local signing	Cloud signing with hash
Slower and less secure	Faster but less secure	Faster and more secure
Whole files must be uploaded and downloaded to the cloud, which slows processing time, expecially with large files, and file transfers are not encrypted	There is no upload or download, so processing is quick. But keys are stored on desktops or local devices, making them more vulnerable to loss or theft	Only the hash is uploaded and downloaded, so transfer speeds are quick, and the full process is protected by encryption. Keys are kept in the cloud, and files are kept locally, so the entire system is secure

DigiCert Secure Software Manager leverages client-side libraries to support hash signing in the following ways:

KSP for Windows

- Supports the signing of Authenticode files with Windows SignTool, Mage, Nuget, Clickonce, HLK, HCK
  - Authenticode file extensions *.EXE, *.DLL, CAB, *.MSI, *.JS, *.VBS, *.PS1, *.OCX, *.SYS, *.WSF., *CAT, *.MSP, *.CPL, *.EFI, *.ARX, *.DBX, *.CRX, *.XSN, *.DEPLOY, *.XAP, and more
- Supports Extended Validation (EV) and Organization Validation (OV) public code signing, as well as private code signing

PKCS11 for Java, Android, Linux, Docker, OpenSSL, GPG, XML, and others

- Supports signing Java file formats (*.JAR, *.WAR, *.SAR, *.EAR) and Android *.APK with JarSigner
- Supports Docker Notary, APIKSigner for Android, OpenSSL, GPG, Debian, XML, JSign, osslsigncode, and more
  - Supports EV and OV public code signing and Private Certificate with 2 5-year duration in order to meet Android requirements for signing

Additional features

With hash signing, you retain the benefit of key protection, user management, and reporting, which Secure Software Manager provides. Secure Software Manager also supports the incorporation of timestamping into your signature as part of your request. This is common for Authenticode, EV code signing, and Java signing.

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

© 2021 DigiCert, Inc. All rights reserved. DigiCert and CertCentral are registered trademarks of DigiCert, Inc. in the USA and elsewhere. Other names may be trademarks of their respective owners.