digicert®

DigiCert Software Trust Manager によるハッシュ署名

ハッシュ署名で迅速かつ容易にコードの安全性を確保

ネットワークの発達した現在、企業とユーザーは、ソフトウェアやアプリのリリースからパッチやアップデートの配布まで、あらゆる場面でファイル共有を利用しています。しかし、コードやアプリを署名する場所がクラウド上や他の署名用の機器になることもあり、その為に未署名のコードを送信したりするのが、従来のコード署名ソリューションでした。

DigiCert Software Trust Manager では、ファイルのアップロードが行われないため、大切な所有物は常に自分の環境に保存されたままです。しかも、ハッシュ署名を利用すれば、鍵の保護やユーザーアクセスといった、ローカル署名にありがちな管理の問題を回避できます。つまり、ローカル署名の迅速さとサービス署名の安全性というそれぞれの利点を活かすことができるのです。

ハッシュ署名の仕組み

1. クライアント側ライブラリ (Windows 用の KSP、Apple 用の Apple CryptoTokenKit、その他のあらゆるプラットフォームに対応する PKCS11 など) が、Software Trust Manager の API とローカル署名ツールとの連係を円滑化します。
2. クライアント側ライブラリは、大きなファイルへの安全な署名を可能にするため、まずリクエストされたアプリケーションのハッシュを生成し、そのハッシュを Software Trust Manager に送信します。そこで、保護された秘密鍵によってハッシュへの署名が行われます。
3. サービスによる署名が終わると、クライアント側ライブラリは署名済みハッシュを署名ツールに返し、そこで署名が元のアプリケーションに統合されます。こうして、元のアプリケーションを組織の外に出すことなく署名が行われます。

主な機能と利点

1. **保護**
   未署名のソフトウェアが組織の外に出ることはありません。
2. **コントロール**
   クライアント側ライブラリはローカル署名ツールとともにコマンドプロンプトによって呼び出します。
3. **サポート**
   Azure DevOps、Jenkins、Apache Ant、Gradle、Apache Maven などの一般的なツールを利用して CI/CD に完全に統合し、署名を自動化します。
4. **管理**
   Software Trust Manager の API と完全に統合され、ユーザーアクセス管理、秘密鍵の保護、およびすべてのコード署名イベントの監査をサポートします。

ファイルによるサービス署名	ファイルによるローカル署名	ハッシュによるサービス署名
遅いが安全	速いが安全ではない	速くて安全
ファイル全体が署名サービスにアップロードおよびダウンロードされるので、特に大きいファイルの場合、処理に時間がかかります。	アップロードやダウンロードが行われないため迅速に処理されます。しかし、鍵が複数の場所に保管されることがある上、その鍵を誰が使っているかを追跡する署名権限の管理機能がありません。FIP 準拠のデバイスに保存されていない場合は、鍵がコピーされたり盗難されるおそれがあります。	ハッシュだけがアップロードおよびダウンロードされるので、転送が高速です。また、処理全体が暗号化によって保護されます。鍵は HSM (Hardware Secure Module) に保存され、ファイルはローカルに保存されたままなので、システム全体が安全です。コードサイニングの標準規格に準拠し、鍵ペアへのユーザーアクセス権のチェックと署名レコードの記録が行われます。

DigiCert Software Trust Managerは、以下のクライアント側ライブラリを利用してハッシュ署名をサポートします。

KSP (Windows 用)

- Windows SignTool、Mage、Nuget、ClickOnce、HLK、HCK での Authenticode ファイルの署名をサポート
  - Authenticode のファイル拡張子 *.EXE、*.DLL、*.CAB、*.MSI、*.JS、*.VBS、*.PS1、*.OCX、*.SYS、*.WSF、*.CAT、*.MSP、*.CPL、*.EFI、*.ARX、*.DBX、*.CRX、*.XSN、*.DEPLOY、*.XAP など
- プライベートコードサイニングの他、EV および OV のパブリックコードサイニングもサポート

CryptoTokenKit (Apple 用)

- Apple のアプリケーションバンドルおよびフレームワークへの署名をサポート。
  サポートするファイルタイプ : *.dmg、*.ipa、*.app
- 署名インストーラパッケージおよびアーカイブとともに使用する Apple productsign をサポート。
  サポートするファイルタイプ : *.pkg、*.mpkg

PKCS11 (Java、Android、Linux、Docker、OpenSSL、GPG、XML など)

- Java ファイルフォーマット (*.JAR、*.WAR、*.SAR、*.EAR) への署名と JarSigner による Android *.APK への署名をサポート
- Docker Notary、Android 用の APKSigner、OpenSSL、GPG、Debian、XML、JSign、osslsigncode などをサポート
- EV および OV のパブリックコードサイニング証明書をサポート。また、Android の署名要件に対応するため、有効期間 25 年のプライベート証明書をサポート。

その他の機能

ハッシュ署名では、鍵保護、ユーザー管理、レポートなど、Software Trust Manager が提供する機能を利用できます。さらに、鍵はオフラインモード、オンラインモードのいずれかを選択できます。オフラインモードでは、鍵の保護と使用の安全性をさらに高めるため、事前承認されたリリース時期に署名するための承認が必要です。また、Software Trust Manager では、リクエストの一環として署名へのタイムスタンプの組み込みもサポートされています。これは、Authenticode、EV コードサイニング、Java 署名では一般的な方法です。

Software Trust Manager についての詳しい情報は、以下のサイトをご覧ください :
https://www.digicert.com/jp/software-trust-manager