

ソフトウェア開発者向けの最新のセキュア ソフトウェアとコードサイニング証明書

DigiCert® Secure Software Managerは、セキュリティを自動化し、コードサイニング証明書の信頼性と使いやすさを実現

従来のコードサイニングの 落とし穴

コードサイニングは、製品開発において、コードの整合性と業界標準へのコンプライアンスを保証するための必須の要件です。従来のコードサイニングと言えば、鍵を共有し、デスクトップ上に鍵を保管し、署名のアクティビティは可視化されていないのが一般的でした。その結果、従来のコードサイニングは鍵の悪用やマルウェアへの不正な署名を引き起こし、それが評判の失墜や経済的な損失につながる恐れがありました。

現在、ソフトウェアやアプリケーションを開発している企業は秘密鍵のセキュリティ、署名アクティビティの追跡、署名と継続的インテグレーション/継続的デリバリー（CI/CD）プロセスの統合に対応するソフトウェアやコードサイニングソリューションを求めています。

Digicert Secure Software Manager とは？

DigiCert Secure Software Manager

コードサイニング鍵の保護を容易にし、コードサイニングアクティビティの役割ベースのユーザーアクセス、監視、管理を実施し、署名をソフトウェア開発プロセスに組み込みます。

署名オプション

ツール、アプリケーション、スクリプト、ライブラリ、プラグイン、その他コンテナ、ファームウェア、メッセージなどの「コード型」のデータも含むあらゆる種類のソフトウェアに署名します。主要なファイルタイプはすべてサポートしています。つまり、保護が必要なすべてのものに署名ができます。

実装オプション

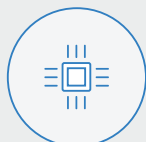
DigiCert Secure Software Managerは、最新のコンテナベースプラットフォームであるDigiCert ONE上に構築され、柔軟な実装オプションを備えています。Secure Software Managerはオンプレミス、クラウド（DigiCert PKIクラウドまたは固有）、あるいはハイブリッドモデルとして実装できます。特殊なユースケースも可能です。



アプリケーション



ファイル



ファームウェア



メッセージ



コンテナ



画像



XML



コード



ソフトウェア



スクリプト

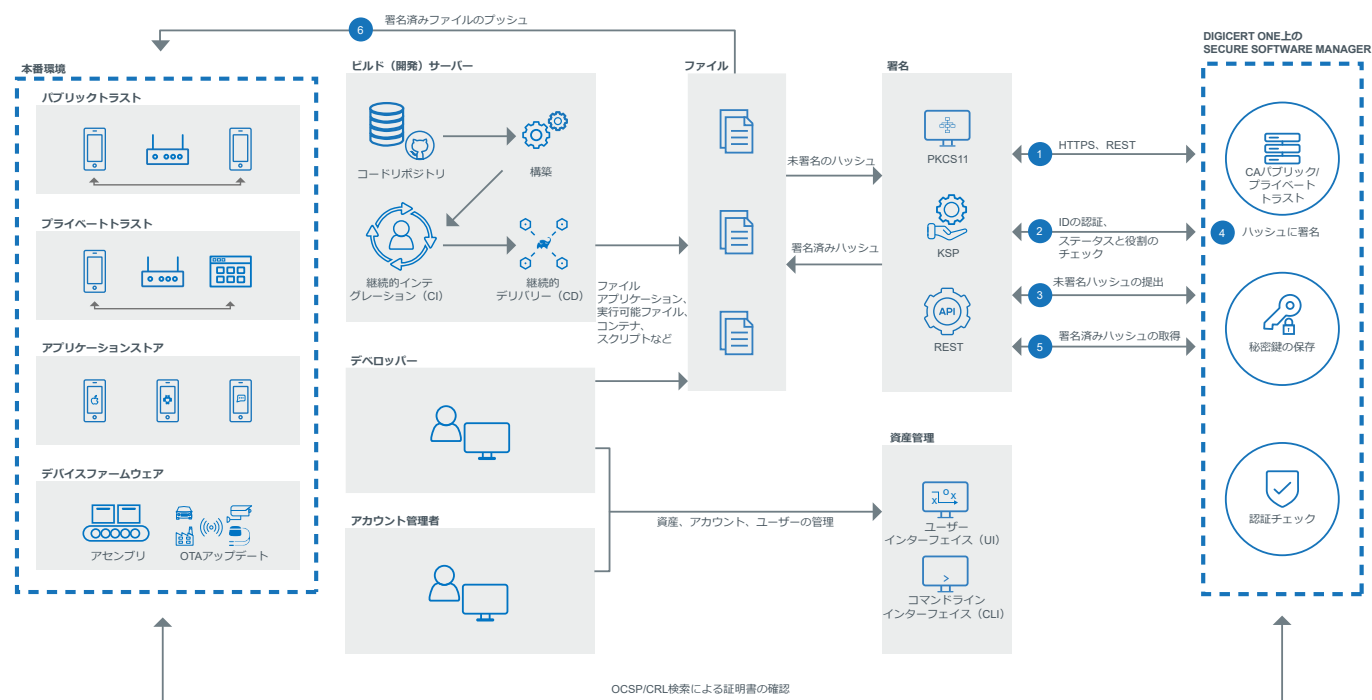
信頼のルート

外部リリース、内部開発、またはその両方に署名するためのパブリックおよびプライベートルート階層を構築します。業界団体の場合は、専用の共有プライベートルートを作成するとエコシステム内でのコードとファイルの配布を信頼できるようになります。自己署名証明書やルート証明書を必要としない鍵ベースの署名を使用するオプションを実行することで、公開鍵を介して検証され保護された秘密鍵署名を配布することができます。

開発プロセス

組み込みAPI統合を使用して、CI/CDプラットフォームでの署名を自動化します。鍵ペアおよび証明書管理、さらにアプリケーションサイニングを使用して、主要なKey Storage Provider (KSP) とクライアント側のライブラリに対するサポートを活用します。ファイルの代わりにハッシュに署名することでセキュリティと速度が向上します。

Secure Software Managerのサイニングワークフロー



メリットと機能の概要

誰がいつ何に署名したかを把握

- 鍵の使用と関連する署名を追跡することで不正使用を回避
- 完全なレポート・監査機能
- 継続使用のために追加の承認が必要な鍵ペア用のオフラインモード

多くのプラットフォームでアプリに素早く簡単に署名

- 有用性とセキュリティを両立するハッシュ署名
- 主要なファイルタイプをすべてサポートするライブラリベースのアプローチ
- 迅速な是正措置のため、過去に遡った証明書の簡単な失効
- 使いやすさを考慮した鍵のインポート/エクスポートに対応したワークフロー
- 短期証明書を利用したテスト署名と期間限定のテスト用鍵ペアをサポート

安全な鍵で署名し、コンプライアンスを保持

- 署名鍵を保護し、署名の使用を制御するための許可ベースのアクセス
- 企業レベルから製品開発までの社内ポリシーの実施をサポートします。これには、署名アルゴリズム、証明書有効期間、プライベートトラスト実装のための異なる拡張鍵使用（EKU）に関するポリシーが含まれます。
- コードサイニング証明書の業界要件を厳守。この要件には、多要素アクセスの実施とパブリックトラストを実装した鍵ストレージ用Hardware Secure Module（HSM）が含まれます。

極めて柔軟でスケーラブルなプラットフォームで成長

- 業界で最も柔軟なソリューションで構築された Secure Software Managerは、オンプレミス、国内、またはクラウド（DigiCert PKI Cloudまたは固有）で実装できます。
- 自動化されたオーケストレーションテクノロジーが、自動的に最適化され、共有されるリソースを使用して一定レベルのパフォーマンスを保持します。
- 迅速な実装が可能で大量（数百万）の証明書への対応が実証済みのインフラストラクチャ

技術仕様

バイナリコードのサポート

- Android
- Authenticode
- ClickOnce
- Debian
- Docker
- GPG
- Java
- Nuget
- OpenSSL
- RPM

Cryptographicライブラリのサポート

- Apple KryptoTokenKit
- Microsoft CNG/KSP
- PKCS#11

継続的インテグレーション/継続的デリバリー（CI/CD）プラットフォームのサポート

- Ant
- Apache Maven
- Gradle
- Jenkins

HSMのサポート

- SafeNet Luna 7
- SafeNet Luna Network HSM

サポートするサービス

- 多要素認証

詳細情報

DigiCertはエンタープライズクラスのSSL、PKI、およびIoTセキュリティソリューションを複数の世界最大手の企業に提供し、常に安心と安全なデータの保護を提供しています。弊社のエキスパートにご相談ください。

詳細については、<https://www.digicert.com/jpl>をご覧ください。