継続的インテグレーション/継続的デリバリーと DigiCert Secure Software Manager

CI/CD プロセスのための最新型コードサイニング

従来型のコードサイニングでは、組織は認証局 (CA) からコードサイニング証明書を購入し、鍵ペアや証明書署名リクエスト (CSR) の作成は組織の責任においてローカルで実施します。したがって、秘密鍵の保護は組織の責任となります。

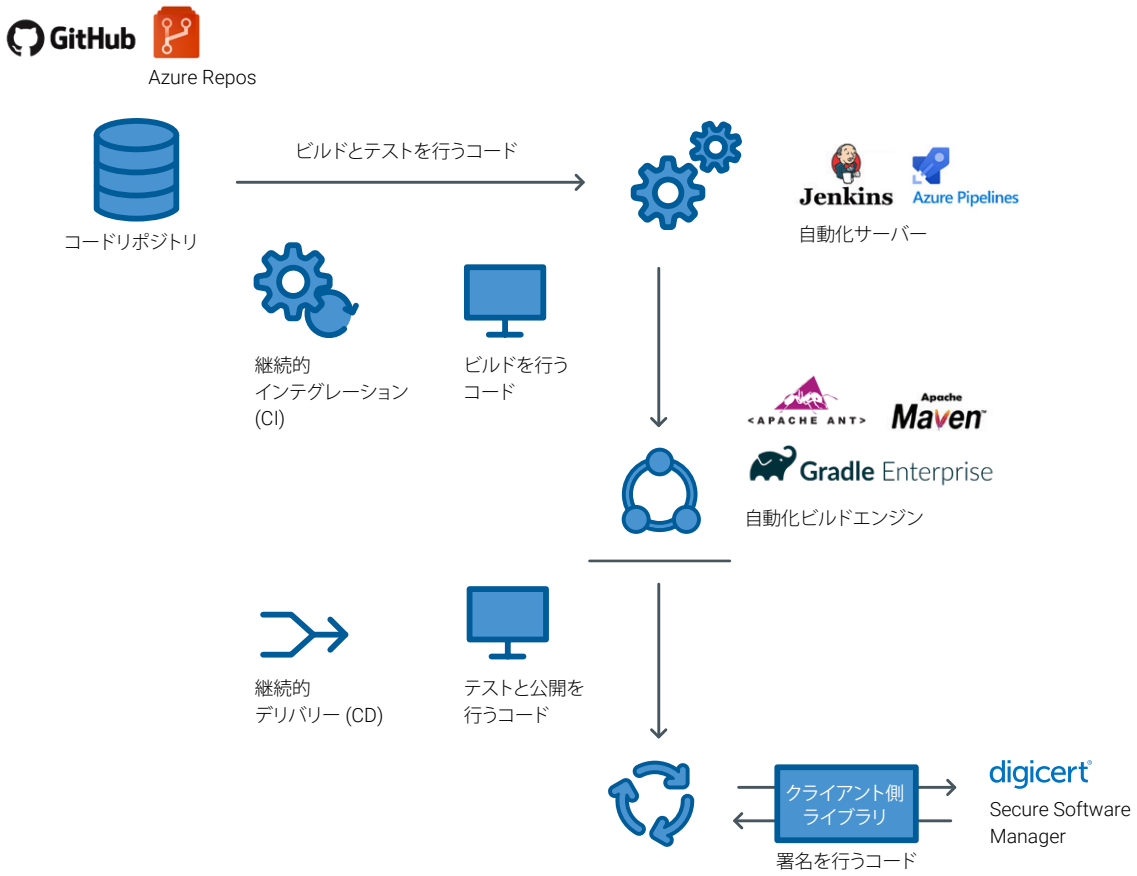
最新型のコードサイニングソリューションでは、鍵ペアをローカルで生成することはせず、その代わり、秘密鍵を安全な場所に一元的に保管し、組織を代表して署名を行う権限を持つユーザーのアクセスを管理します。

従来型のコードサイニングでは、ソフトウェア開発チームは安全性と生産性のどちらかを選ばなければなりません。共有の鍵、もしくはデスクトップや保護されていないデバイスに保管された鍵を使用して、その場ですばやくコードに署名を行います。このような鍵は盗まれたり悪用されたりしやすく、コードに署名してマルウェアを拡散させるのに使われるおそれがあります。そうなると、あたかも組織がマルウェアを拡散しているかのように見られてしまいます。

最新型のコードサイニングでは署名鍵の安全性が確保されるため、開発者は鍵の保護に関する負担から解放されます。また、最新型のコードサイニングは開発者の CI/CD プロセスにシームレスに統合することができます。そのため、高い生産性を維持しながらコードサイニングのベストプラクティスを実践することができます。

コードサイニングの利便性と効率性を高める Secure Software Manager

コードサイニングとは、署名が行われた時点以降、そのコードが改変されていないことを保証するものです。コードの完全性を確保するため、品質保証試験と製品出荷の前に、PKI の証明書によって、暗号化、認証、身元確認を実施します。次の図に示すように、最新型コードサイニングソリューションである Secure Software Manager を利用すれば、DevOps チームは使用している自動ビルドツールに安全で高性能なコードサイニングをシームレスかつ容易に組み込むことができます。



アジャイル開発のための自動コードサイニング

- Apache Ant、Apache Maven、Azure DevOps、Gradle、Jenkins などのメジャーな CI/CD プラットフォームに暗号化サービスプロバイダ (CSP) を直接統合できるようにすることで、署名を自動化します。
- CI/CD パイプライン内から自動的に呼び出すことができる、スクリプトによる統合のためのデジサートのクライアント側ライブラリ (Microsoft KSP、Apple CryptoTokenKit、PKCS11) を活用し、オーバーヘッドを最小化します。
- 複雑なユーザー操作を必要としない、再現可能なコードサイニングのベストプラクティスを採用しています。

開発者の負荷を増やすことなくコードサイニング証明書によるセキュリティを強化

- 使い捨て鍵やオンデマンド鍵など、複数の鍵署名モデルの選択肢を利用してセキュリティを最大限高めた場合でも、開発者のセキュリティに関する負担は軽減されます。鍵署名モデルは、メジャーな署名プラットフォームやユーザーのニーズに合ったものを用意しています。
- 許可ベースのアクセスにより、安全なアクセスと、署名や管理の権限を維持します。人事異動があった場合にも、集中型のコントロールパネルからアクセスレベルを迅速かつ安全に変更できます。ビルドサーバーを API ユーザーとして設定できるため、人の手を介さず署名リクエストを実行できます。
- 署名済みコードやアクティビティを追跡する詳細なレポートやログを簡単にエクスポートできます。プロセスをさらに自動化するため、API を介してレポートや監査をリクエストすることも可能です。
- 将来的にはタイムスタンプによる時間ベースの検証にも対応します。

大規模開発にも対応する性能の高さ

- 署名の際に実際のソースファイルをクラウドに転送する必要がない「ハッシュ」署名を行うことで、サイズの大きなファイルの署名を効率よく処理します。
- パブリックな EV および OV のコードサイニング、プライベートコードサイニングに加え、Microsoft Authenticode、Java、Android、Docker など、主要なすべてのバイナリタイプにも対応するハッシュ署名により、大規模開発の効率を向上させます。

Secure Software 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/signing/secure-software-manager/