一目でわかる

digicert

スムーズで安全なコードサイニングのための DevOps ガイド

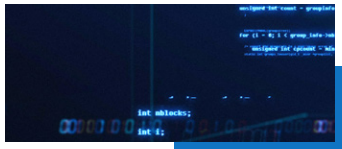
かつて、安全な署名は DevOps の障壁となっていましたが、今は違います。この新しい手法が、開発/リリースするソフトウェアを保護する最高の（スムーズな）方法である理由を説明します。

過去	現在
• 手作業による署名 • 鍵の共有 • プロセスの不一致 • 不十分な可視化 • 是正が困難	• 自動署名ワークフロー • 鍵は HSM に保管 • アクセス制御 • 一元的トラッキング • 迅速な是正

今までの手法の問題点とは

かつて、ソフトウェア署名は手間がかかって管理が難しいだけでなく、ソフトウェアリリースプロセスのセキュリティギャップでもありました。手作業による署名手法には手間がかかるため、署名はソフトウェア開発プロセスの足をひっぱる苦行であり、多くの人がこの重要な手順を省略する結果となっていました。コーディングがスクリプト化されていなかったため、エンジニアは適切な署名ステージのために開発ステップを延々とモニタリングし続ける必要がありました。

セキュリティ自体について言えば、今までの手法は時間がかかって手間取るだけでなく、強力なセキュリティを提供できないという問題もありました。ローカルに保管された証明書は盗まれたり、紛失されたり、不正使用されるリスクがあります。秘密鍵は追跡、管理できないため、個人が署名すべきでないときに署名したり、監督されることなく鍵を共有したりする可能性があり、監査と是正は困難または不可能でした。



署名はよりシンプルに、より安全に

現在、署名は CI/CD パイプラインに統合可能になり、ほぼ何の手間もいらなくなりました。デジサートではこれを「継続的署名」と名付けました。自動化されたプロセスにより、手動で監視する必要がなく、適切な段階で署名が確実に行われます。スクリプト化されたツールにより、開発段階全体で署名マネージャーによって継続的に署名プロセスが実行されるため、エンジニアは設計、コーディング、フィードバックに専念できます。

また、この新しい署名手法はエンジニア、チーム、組織を不正使用やミスから守りながら、最高レベルのセキュリティを提供します。鍵は HSM または署名ソリューションツールに保管されるため、紛失、盗難、不正な共有やアクティビティから守られます。マネージャーやチームリーダーは、証明書と DevOps の鍵の使用状況を簡単に監視、監査し、問題が発生したときはそれを是正できます。

スムーズな道は安全な道

署名がスムーズかつ安全になると、エンジニアは署名に気を取られることなく、素晴らしいソフトウェアの開発に専念できるようになります。ソフトウェアサプライチェーン攻撃が増加する今、ソフトウェア署名は継続的デリバリーに不可欠な要素であるため、このことは重要です。デジサートの継続的署名を利用すれば、エンジニアは開発を中断することなくコードを保護できます。

ソフトウェア署名の自動化に興味をお持ちですか?
digicert.com/jp/signing/secure-software-manager をご覧ください。