digicert®

DigiCert Secure Software Manager による専用プライベート認証局

長寿命デバイスの信頼の有効期間を完全に制御する

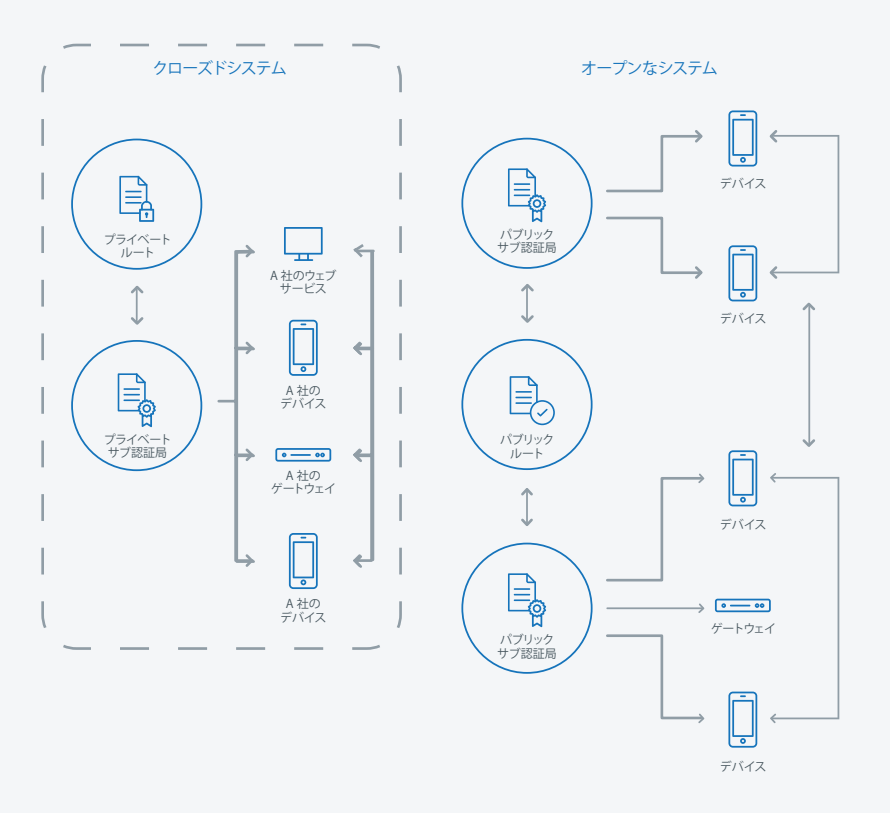
工業、医療、自動車などの産業で用いられる多くの機械や装置には、独自の信頼性要件があります。これらの用途では、多くの場合、基準の要件よりも有効期限を長くする必要があります。また、デバイス上で信頼性を確認する必要があります。そのため企業では、寿命の長いデバイスや IoT デバイスへのアップデートや署名、コードの配布を、プライベート階層サービスを利用してカスタマイズし、管理しています。

DigiCert Secure Software Manager による専用プライベート認証局

DigiCert Secure Software Manager が提供する専用プライベート認証局ソリューションを利用すれば、プライベートルートから、中間証明書、エンドエンティティ証明書まで、信頼のチェーン全体を管理することができます。強力なマネジメントソリューションによって、可視性、俊敏性、柔軟性、そして安全性が得られます。

また、専用プライベート認証局があれば、パブリックな信頼の機能を補完するプライベート証明書の管理も可能になります。自前の認証局のために初期費用をかけずに、安全な鍵管理とユーザー管理を維持しながら、すべての配布をコントロールできます。さらに、パブリックな EV コードサイニング証明書の場合と同様、署名鍵を FIPS (Federal Information Processing Standard: 米国連邦情報処理標準規格) 140-2 に準拠する HSM (Hardware Security Module: ハードウェアセキュリティモジュール) に保存することもできます。

企業のプライベートな信頼とパブリックな信頼の例



主な利点

- 最先端の保護技術により、署名サービスの鍵を安全に保管。HSM も選択可能
- リリース毎に異なる秘密鍵と証明書で署名ができる固有の鍵を配布することによって俊敏性を維持
- エンドエンティティ証明書の有効期間を柔軟に設定できる、専用のプライベート CA を使用
- 特定のアプリケーションのコードに署名できる人、証明書を発行できる人、証明書発行時にパラメータを設定する人といった制御が可能
- コードサイニングのあらゆるアクティビティが可視化され、詳細な情報を管理
- 既存のツールとの統合が容易
- 証明書を失効させる必要がある場合、影響が最小限に制御
- ウェブまたは API 経由のアクセスによって、どこからでもアクティビティを管理
- コマンドラインのインターフェイスやコントローラの使いやすさが向上し、権限のあるユーザーがコマンドラインから鍵ペアや証明書を生成・管理
- 署名鍵の保管方法を複数のオプションから柔軟に選択
- 既存の鍵、証明書、ICA、ルート証明書を簡単にインポートでき、署名アクティビティを一元化

サポート

DigiCert Secure Software Manager は以下のような幅広い種類のファイル形式をサポートし、ファームウェアや IoT デバイスアプリケーションへの署名を可能にしています。

- Debian
- Docker Notary
- GPG
- OpenSSL
- RPM
- XML
- PKCS11、Microsoft KSP、Apple CryptoTokenKit と互換性のあるあらゆる署名ツール

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/