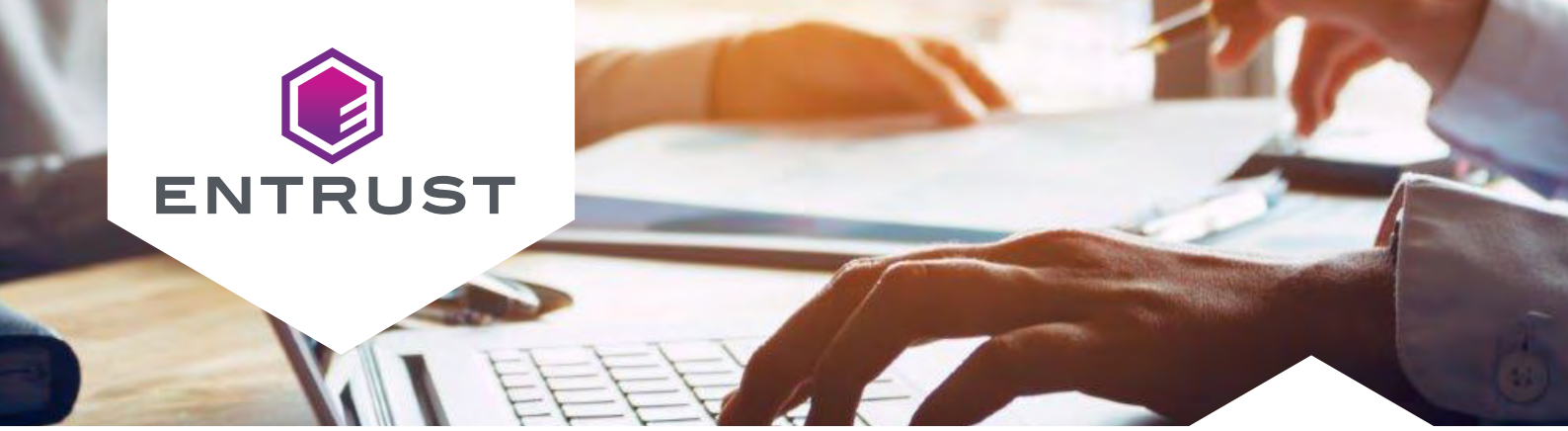

Entrustコード署名ソリューション

コード署名のための高保証セキュリティ

ハイライト

- 作成者、発行日、コンテンツの保護
- ソフトウェアの整合性の確立
- 重要なコード署名鍵の保護

コード配信における課題

ビジネスITは複雑で、組織を運営するために幅広いソースからのソフトウェアを使用しています。ソフトウェア開発会社は、社内使用または顧客への販売を問わず、ソフトウェアの真正性を証明するメカニズムを構築またはサポートする必要があります。このセキュリティを確保するには、以下が必要です。

- 署名プロセスを検証することによって、正しいコードを正しい鍵で署名する
- 秘密署名鍵を管理して盗難を防ぎ、不正なバージョンが顧客に届かないようにする
- すべての署名活動の監査証跡を提供する

Entrustは安全なコード署名ソリューションの開発・実装における重要な専門知識を備えています。このソリューションは次の機能を提供することで、プロセス、整合性、認証、秘密鍵の保護の課題を解決します。

- 主要な盗難、企業の「なりすまし」、悪意のあるソフトウェアの改ざんのリスクを軽減する
- エンドユーザーがソースとソフトウェアの整合性を確認し、変更または悪意のあるコードの挿入を検知できるようにする
- 署名されていないソフトウェアに対するOSの強力な警告ダイアログが表示されるため、ユーザーがインストール放棄するのを防ぐ
- コード署名操作のためのアクセス制御、承認ワークフロー、自動化、監査機能を提供する

これらの機能を提供するために、Entrustは、信頼の基点としてnShield®ハードウェアセキュリティモジュール（HSM）に基づく2つのコード署名ソリューションを提供します。

これらのソリューションとは？

- Code Signing Gateway
- HSMとの直接統合によるコード署名

コードとは

コードは、ターゲットプラットフォームによって使用または実行される情報のバイナリパッケージとみなされます。コードの例には、実行可能パッケージ、インストーラーパッケージ、ファームウェアパッケージ、組み込み環境が含まれます。

詳細をチェック：ENTRUST.COM/ja/HSM

Entrustコード署名ソリューション

信頼の基点としてEntrust HSMを使用したコード署名

コード署名は、ソフトウェア発行に対するデジタル署名に適用されます。コード署名を使用することで、エンドユーザーは発行者のIDを認証し、ソフトウェアのソースと整合性を検証することができます。また、OSが署名されていないソフトウェアに対して強力な警告ダイアログを表示するため、ユーザーがソフトウェアのインストールを放棄するのを防ぎます。

コード署名ソリューションは、ソフトウェア発行者の公開鍵・秘密鍵のペアとデジタル証明書を使用します。デジタル証明書はソフトウェア発行者の公開鍵を含み、適切なCAによって署名され、エンドユーザーがコードを検証できるようにします。このプロセスは、ソフトウェア発行者が配信するコードをハッシュ化し、その秘密鍵を使用してハッシュ値に署名／を暗号化したときに開始されます。その後、暗号化されたハッシュ値と元のコードをデジタル証明書とともに、パッケージでエンドユーザーに配信します。最終ステップとして、エンドユーザーはソフトウェア発行者の公開鍵を使用して、暗号化されたハッシュコードを復号化し、結果のハッシュ値を受信したコードの再生成されたハッシュ値と比較します。ハッシュ値が同一の場合、コードが検証されます。

nShield 汎用HSM

nShield HSMは、様々なアプリケーションで使用される鍵を生成かつ保護するための安全な環境を提供する、強化された、認定改ざん防止デバイスです。また、サービスとして利用可能なnShield HSMは、次の3つのフォームファクタで利用できます。

- **nShield Connect**はネットワーク全体で複数のアプリケーションに対応するアプライアンスであり、サービスとしても利用可能です。
- **nShield Solo**、単一サーバ上のアプリケーションに対応するPCIeカード
- **nShield Edge**、少量のトランザクション用のUSB接続型デスクトップデバイス

nShield HSMは、FIPS 140-2レベル2およびレベル3認証を受けています

秘密鍵はコード署名システムのセキュリティにとって非常に重要であり、決して公開または共有してはいけません。秘密鍵が損なわれると、信頼システムは機能しません。秘密署名鍵のセキュリティは、コード署名プロセスを支えています。

コード署名などの機密性の高いアプリケーションの場合、安全なソリューションの作成には、使用時と非使用時の両方で秘密鍵を保護することが重要です。HSMは、ライフサイクル全体で鍵を保護する、認定された改ざん防止環境を提供します

Code Signing Gateway

高度制御されたソフトウェア署名承認プロセスを必要とする大規模な組織に対して、Code Signing Gatewayは、ソフトウェア開発組織が強力なセキュリティ要件を満たすのに役立つ、柔軟で一元化されたワークフロー自動化機能の範囲を提供します。Code Signing Gatewayは、Entrustコード署名ワークフローアプリケーションを実行する、顧客ホストの集中サーバです。

Code Signing Gatewayは、ワークフロー管理、要求の受け入れ、Eメールでの承認者への通知、タイムアウト管理、承認の確認、アクティビティのログへの記録、署名されたコードのステージングエリアへの移動を行います。次のような複数のユーザーの役割のサポートが可能です：Code Signing Gateway管理者、エンタープライズ、デスクトップ、IoTまたはモバイルアプリケーション開発者、管理チーム、コード署名承認者など。Active Directory統合は、ワークグループの承認とユーザーの認証に使用されます。

詳細をチェック：ENTRUST.COM/ja/HSM

Entrustコード署名ソリューション

nShield HSMは、コードの署名に使用される秘密鍵の保護に使用されます。署名鍵はHSM内部に格納され、Code Signing Gatewayで作成できる複数の署名プロファイルにマップされます。

Code Signing Gatewayは、Oracle Jarsigner、Microsoft SignTool、Appleコード署名ツール、Androidのコード署名ユーティリティなどのスタンダード署名ツールと統合されます。プロセスの概略図を図1に示します。

追加機能には、複数の署名プロファイルをサポートする多数のデジタル証明書を使用するために定義づけできる複数の署名プロファイル、集中ログ、ファイルアーカイブ、タイムスタンプサービスとの統合、署名前にファイルのウイルスチェックのためのMicrosoft Defenderとの統合が含まれます。

Entrust Code Signing Gatewayは、Entrust専門サービスチームによって、各顧客に固有の環境に合わせてカスタマイズされたソリューションです。

HSMとの直接統合によるコード署名

nShield HSMとの直接統合は、少数の開発者向けのソリューションに業務の簡単な分離を提供します。これは通常、個別の開発者ワークステーションまたは専用のコード署名サーバに使用されます。コード署名に使用される秘密鍵は、nShield HSMによって生成かつ保護されます。

コード署名は、Java Cryptography Extension (JCE)、Microsoft CAPI、CNGどの標準APIを使用してHSMと統合し、Jarsigner、SignTool、OpenSSLなどのサードパーティツールを使用して、HSMで実行する署名要求を作成します。

詳細

Entrust nShield HSMの詳細については、**entrust.com/ja/HSM**をご覧ください。アイデンティティ、アクセス、通信、データに関するEntrustのデジタルセキュリティソリューションの詳細については、**entrust.com/ja**をご覧ください。

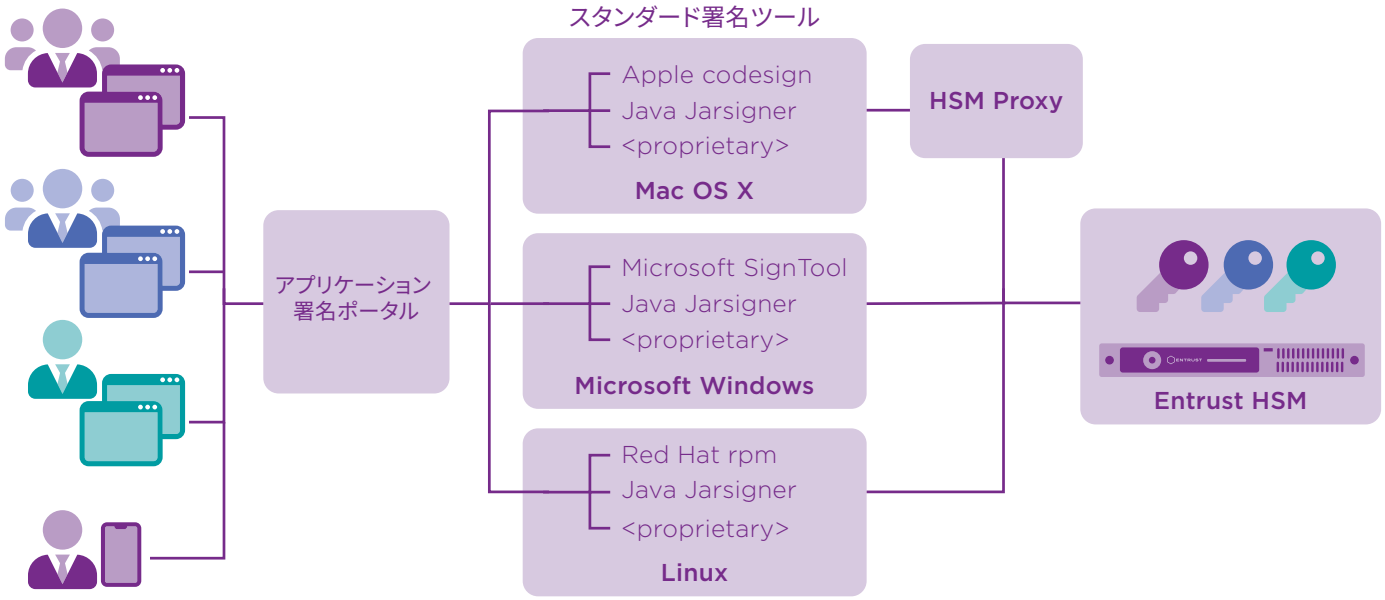

Figure 1: Code Signing Gateway schematic

Entrust nShield
HSMの詳細はこちら:

HSMinfo@entrust.com

entrust.com/ja/HSM

ENTRUSTについて

Entrust は信頼できる認証、支払い、データ保護を実現することで、動き続ける世界をセキュアにしています。今日、支払いや国際取引、電子政府サービスへのアクセス、そして企業ネットワークへの認証において世界中でより安全で円滑なユーザ体験が求められています。Entrust はこれらの要となる部分において、他に類を見ない幅広いデジタル セキュリティとID発行ソリューションを提供しています。2,500人を超える従業員、グローバルパートナーネットワーク、そして150カ国以上におよぶ顧客に支えられ、世界で最も信頼されている組織から信頼されています。

詳細は下記URLをご覧ください:
entrust.com/ja/HSM

お問い合わせ:
HSMinfo@entrust.com