Symantec™ Secure App Service

ビジネスの完全性を保護する、他に類を見ないコード署名鍵セキュリティ

Symantec™ Complete Website Security

データシート

ソリューション概要

Symantec™ Secure App Service は、コードサイニングの不適切な管理による、重大な財務的影響やブランドダメージからビジネスを保護します。コードサイニングに対する視認性、敏捷性、そして信頼できる安全性を提供し、お客様の不安を払拭します。当社は鍵をミリタリーグレードのデータセンターで保護します。お客様はコードサイニングのすべての処理を完全に制御し、またすべての情報を把握することによって、アプリケーションを保護し、安心して販売することができます。

Secure App Service により、あらゆる対象プラットフォームで、よりシンプルで高度なコードサイニングを実施できるようになります。サイバーセキュリティの世界的リーダーである、当社のセキュリティ、サービスおよびサポートは信頼性が高く、お客様のビジネスやコードサイニングの取り組みを保護することができます。

ホスティングサービスによる安全な鍵の保管

鍵はすべてシマンテックのミリタリーグレードのデータセンターにて保管

複数の署名サービス

ローテーション鍵、オンデマンド鍵、固有鍵を利用可能

ロールベースのアクセス制御

ロールの変更に合わせて SAS へのアクセス権も変更される、高度なアクセス制御

完全なレポートおよび監査ログ

アクセス権限、ロール、署名イベント処理および署名済コードについての情報を確認できる高度な視認性

Symantec Secure App Service は、コードサイニングに関するあらゆる管理サービスを提供し、ビジネスとユーザーを保護します。

Secure App Service では、お客様の社内環境でアプリケーションに署名するのではなく、当社の安全なクラウドサービスにアプリケーションをアップロードしていただいて署名を行います。これにより、証明書の秘密鍵を、ミリタリーグレードのデータセンターに安全に保存することができます。当社の重要な PKI で使用しているのと同じインフラ、同じスタッフによって、お客様にも障害復旧やストレージ、高い拡張性や性能を提供します。これにより、署名の処理が簡素化・迅速化されるうえ、鍵を社内環境に保存する場合に生じるセキュリティリスクや管理の複雑さが緩和され、ハードウェアセキュリティモジュール（HSM）への投資も不要となります。

また、セキュリティポリシーやファイルサイズなどの理由により、バイナリコードを当社のサービスにアップロードできない場合、代わりにコードのハッシュ値をアップロードして署名するハイブリッドモデルを提供しています。

多くのソフトウェアベンダー、OS ベンダーが想定する主要なコード署名モデルはすべてサポートしていますので、ターゲットプラットフォームと社内セキュリティーポリシーの要件に適合する署名モデルを容易に選択できます。署名モデルには、固有鍵モデル、オンデマンド／複数鍵モデル、ローテーション鍵モデルの 3 種類があります。特定の署名サービスを選択すると、お客様側で別のモデルを選択しない限り、ターゲットプラットフォームに最も適した署名モデルが自動的に使用されます。

主な特長

コードサイニングの視認性

Symantec Secure App Service では、コードサイニング処理がすべて可視化されており、詳細な情報を得ることができます。また、当社はミリタリーグレードの保護を備えたクラウドに鍵を保存しているため、鍵がどこにあり、安全であるかどうかを常に把握できます。

- 鍵が安全であり、会社の評判が守られていることがわかります。
- 誰が何に署名したかを把握できます。
- 鍵を共有できないようにすることで安全性を確保し、アプリケーションを守ります。
- コンプライアンスを維持します。

敏捷性と管理機能

Symantec Secure App Service は汎用性が高く、さまざまな種類のプラットフォーム上でアプリケーションへのコードサイニングを容易に実行できます。

- より多くのプラットフォーム上で、より迅速に、アプリケーションへのコードサイニングを実行できます。
- ビジネスの重点的な取り組みにリソースを振り向けることができます。
- アプリケーションへのコードサイニングを実行できるユーザーを管理できます。
- 証明書を取り消す必要がある場合、影響を最小限に留めます。

コードサイニングの安全性

Symantec Secure App Service により、コードサイニングの鍵の安全性を確保しつつ、社内のセキュリティポリシーに則って鍵を使用することが可能となります。

- ビジネスを財務的損害や評判の失墜から守ります。
- アプリケーションの寿命と完全性を維持します。
- すべての人が事前定義された基準に従って署名します。
- マルウェアを含む可能性のあるアプリケーションへの署名を防止します。
- 顧客のより強い信頼を育みます。

Symantec

Symantec™ Secure App Service

ビジネスの完全性を保護する、他に類を見ないコード署名鍵セキュリティ

Symantec™ Complete Website Security

きめ細かいロールベースのアクセス制御により、コードサイニングサービスに誰がアクセスでき、どのような操作を実施でき、どのコードに実際の署名が行われるかを制御できます。個人に割り当てられたロールが変更されれば、必要に応じてアクセス権の取り消しや修正が行われます。

Secure App Service は、ウェブポータルによる包括的な鍵管理を提供します。さらに、当社のコードサイニングサービスをお客様の既存の社内システムとワークフローに統合し社内の処理を自動化するための API も提供しています。

Secure App Service を利用すると、コードサイニングのすべての処理と鍵について、記録、レポート、監査を行うことができます。したがって、いつ誰がどのアプリケーションの署名を依頼したかがわかります。また、鍵の有効期限が通知されるので、事前に新しいアプリケーションバージョンに更新することができます。

Secure App Service は定額サービスですので、作成した証明書の数ではなく、コード署名イベントに対してのみ支払いが発生します。年内に想定されるコード署名回数に対して一定額を支払うことができます。固有鍵やローテーション鍵を使用してセキュリティの強化を図っても、追加費用は発生しません。鍵はクラウドに安全に保存されるため、ハードウェアセキュリティモジュール（HSM）などの特別なセキュリティハードウェアに投資する必要がありません。

機能概要

クラウドベースのコードサイニングサービス

- コードサイニングを簡素化および迅速化します。
- セキュリティリスクを最小化します。
- コードサイニングの管理機能の不足、管理の複雑さ、適切な制御を可能にするための HSM への投資など、社内でコードサイニング処理を行う場合に生じる問題点を解消します。
- 障害復旧やストレージ機能、高度な拡張性や性能がはじめから提供されます。

複数のコードサイニングモデル

- 主要な OS ベンダー要件をサポートします。
- 社内コンプライアンスポリシーにも柔軟に対応します。
- 最も安全で最も適切なコード署名モデルを使用することが容易になります。

ロールベースのアクセス制御

- セキュリティリスクを最小化します。
- 業務中断を回避します。
- コードサイニング処理を制御します。
- 説明責任とコンプライアンスを強化します。
- ビジネスクリティカルなコード署名鍵へのユーザーアクセスを制限します。

ウェブポータルおよび API を利用した管理

- コードサイニングの管理を簡素化します。
- 社内の手動処理を自動化し統合します。
- どこからでもコードサイニングの処理を行えます。
- 社内でのビルドプロセスに合わせてコードサイニングのテストと本稼働を実施できます。

Symantec

Symantec™ Secure App Service

ビジネスの完全性を保護する、他に類を見ないコード署名鍵セキュリティ

Symantec™ Complete Website Security

現在使用可能なサイニングサービス

Adobe PDF	.pdf
Android	.apk (ZIP 調整最適化を含む)
Android アサーション	.apk
EV コード署名	Microsoft Authenticode で参照されるファイルを使用
GPG	すべてのファイルタイプ
Microsoft Authenticode Hash	Microsoft Authenticode で参照されるファイルを使用
Java	.jar、.war、.ear、.sar
Java モバイル	.jar および .jad (両方とも必須)
LISP	現在利用可能
Microsoft Authenticode	.exe、.dll、.cab、.msi、.js、.vbs、.ps1、.ocx、.sys、.wsf、.cat、.msp、.cpl、.ef1
Microsoft XAP	.xap
Microsoft CAB	.cab
OpenSSL	すべてのファイルタイプとすべてのファイルハッシュ
RPM	.rpm
SHA-1 署名	レガシー OS (MS Windows Vista および Server 2008) 用
XML – DISG 準拠	.xml
XML – XAdES-T フォーマット	.xml、.docx、.xlsx、.pptx (Office 文書)

サポートされるタイムスタンプサービス

RFC 3161:SHA1 および SHA256
Microsoft Authenticode
Adobe PDF

監査ログによる説明責任およびコンプライアンスのレポート

- CISO やセキュリティ管理者に対し、説明責任やコンプライアンスを示すことができます。
- 誰が、何にいつ、何度署名したかがわかります。
- すべてのコードサイニング処理を容易に記録しモニタリングすることができます。
- リスク分析、予測、およびリソース管理に役立つ情報やデータが得られます。

柔軟で低価格な定額サービス

- 柔軟な年間定額制により費用を抑えられるので安心です。
- 固有鍵、ローテーション鍵を使用しても追加費用がかかりません。
- HSM などのハードウェア投資費用を不要にします。

Symantec™