Secure App Service（SAS）で使用する暗号鍵モデル

Symantec SAS – エンタープライズクラウドベースの署名サービス

Symantec™ Complete Website Security

DATASHEET

Symantec Secure App Service (SAS) は、主要なソフトウェアおよびオペレーティングシステムのベンダーによって要求される3つの署名モデルをサポートしています。

#1: Unique keys（固有鍵）

これは、シングルユーズモデルとも呼ばれます。

このモデルでは、署名イベントごとにその場で新しい証明書が作成されます。この場合、ファイルまたはファイルのグループは、証明書と署名イベント（ファイルが署名のために提出される）の間で1対1の対応関係を持ちます。秘密鍵は1回だけしか使用されないため、危険にさらされることはありません。取り消しが必要になった場合も、他のアプリケーションには影響しません。これは、最も安全な署名モデルです。このモデルは、Javaファイルの署名に使用されます。

#2: On-Demand Keys（オンデマンド鍵）

これはまた、「オンデマンドプール」モデルとも呼ばれます。

暗号鍵はプール内に保持され、わかりやすいフレンドリネームが割り当てられます。

署名の申請をおこなう場合、既存の証明書を選択するか、新規作成することができます。

Android OS（アプリケーションなど）で使用するファイルに署名する必要がある場合、Androidではアプリケーションのリリースのたびに同じ証明書を繰り返し使用することを要求するため、このモデルが最適です。そのため、署名サービスに関連付けて署名証明書の番号が提供されます。

#3: Pool of Rotating keys（ローテーション鍵）

このモデルでは、Microsoft SmartScreenフィルターの評価モデルがサポートされます。Microsoft OSで使用するファイル（DLLファイル、EXEファイルなど）に署名する必要がある場合、Microsoftでは、署名に同じ証明書を繰り返し使用するのではなく、プール内の証明書を循環して使用することが要求されます。秘密鍵は、必要に応じてオンデマンドで生成され、決められた期間内（1日、8日、または15日）は同じものを使用する必要があります。有効期限に達すると、他の暗号鍵が再使用されます。

Microsoftでは、このモデルを使用する開発元に高いレベルの認証を要求しています。そのため、当社ではすべてのMicrosoftベースの署名サービスにこれを実装しています。

Windows, OpenSSL および Java のアプリケーションへの高速署名(Hash Signing Service)

Symantec Secure App Serviceで大規模なアプリケーションを署名する場合、Secure App Serviceクラウドにアップロードせずに、署名を行うことができます。

このソリューションは、当社のAPIおよびインストールされているローカルアプリケーションと連携し、署名が要求されているアプリケーションのハッシュ値を計算し、クラウドで署名を行うSASにその値を渡すやり方で、サイズの大きなファイルの署名を実行します。

ハッシュが署名されると、SASはローカルアプリケーションにハッシュを送り返し、ローカルファイルに追加することで、アプリケーションが署名されます。

SASが提供する秘密鍵の保護、ユーザー管理およびレポート作成のメリットはそのままです。

SASにアップロードされるのはファイル全体ではなく、ファイルのハッシュだけであるため、SASに含まれているマルウェアスキャンニングサービスは高速署名(Hash Signing Service)では使用できません。

関連サービス

Symantec Secure App Service (SAS)[1]は、当社のComplete Website Security (CWS)ソリューション[2]の一部です。

[1] https://www.symantec.com/code-signing/secure-app-service/
[2] https://www.symantec.com/complete-website-security/

Symantec

Secure App Service（SAS）で使用する暗号鍵モデル

Symantec SAS – エンタープライズクラウドベースの署名サービス

Symantec™ Complete Website Security

どの署名モデルが必要ですか？

どのモデルを使用するかは、要求された署名サービスだけでなく、その会社独自の要件やポリシーにも依存します。たとえば、オンデマンド署名モデルは、通常Androidアプリに使用されますが、他の種類の署名サービスにも使用することができます。

「デフォルト」で使用するものが必要な場合は、以下のモデルをお勧めします。

- Javaファイル：Unique keys
- Androidファイル：On-demand keys
- Microsoftファイル：Rotating keys
- 他のファイル（デフォルト：Unique keys）

SASでは、すべての署名モデルがデフォルトで有効にされています。署名サービス（Authenticodeの署名など）を選択すると、プラットフォームが自動的に適切なモデル（この例では、回転キーのプール）を選択してくれます。自社のニーズに合わせ、セキュリティの強度を最大化するために、この署名サービス自動選択の設定を変更することができます。

完全なコントロール、リスクの低減、コストの削減

マネージド PKI for SSL は、お客様の SSL サーバ証明書に対する重要なセーフティネットを提供します。一元管理とコントロールを行うことにより、何かを見逃したり忘れたりという危険がなくなり、また、お客様の Web サイト により優れたセキュリティを追加します。

シマンテック コンプリート Web サイト セキュリティのご契約、または、お客様の SSL サーバ証明書管理にシマンテック コンプリート Web サイト セキュリティがどのように役立つかについてお知りになりたい場合は、下記までご連絡ください。

合同会社シマンテック・ウェブサイトセキュリティ

https://www.jp.websecurity.symantec.com/
〒107-0052　東京都港区赤坂1-11-44 赤坂インターシティ
Tel : 03-5114-4137
E-mail : mpki-ssl_jp@symantec.com

Symantec™