Secure App Service（SAS）で使用する暗号鍵モデル

DigiCert SAS - エンタープライズクラウドベースの署名サービス

DigiCert 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、シングルユース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（このイベント時に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、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。署名の申請を行う場合、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。

MicrosoftOS 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。

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よっても異なります。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。

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

Windows、OpenSSL、および Java のアプリケーションへの高速署名

DigiCert 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て、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ニングサービスは高速署名では使用できません。

関連サービス

DigiCert 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。

詳細については、IoT エキスパート（JPN-DIV-MPKI@digicert.com）にお問い合わせください。

リーハイ

2801 North Thanksgiving Way Suite 500
Lehi, UT 84043
USA

マウンテンビュー

487 E. Middlefield
Buildings K & J
Mountain View, CA 94043
USA

英国

88 Wood Street, Suite 1001 & 1002
London EC2V 7RS England

スイス

Balexert Tower, 18 Avenue Louis-Casai
Unites 01 and 30CH-1209
Geneva, Switzerland

ケープタウン

Gateway Bldg. (3rd, 4th, & 5th floors)
Century Blvd & Century Way 1
Century City, Cape Town 7441
South Africa

オーストラリア

437 St. Kilda Road
Level 3, Unit 4.01
Melbourne VIC 3004
Australia

中国

23F/Taikang Financial Tower
38 East Third Ring Road
Chaoyang District, Beijing, 100026
China

日本

〒 104-0061
東京都中央区銀座 6 丁目 10 番地 1 号
GINZA SIX 8 階

インド

10th Floor-RMZ Eco World, Sarjapur,
Marathalli Outer Ring Road
Devarabeesanahalli Village
Bangalore, India 560103

digicert® | Symantec™ Website Security