

Symantec Secure App Service (SAS) supports three signing models that are requested by major Software and Operating System vendors.

#1: Unique keys

This can also be referred to as a single use model.

In this model we create a new certificate on the fly for each signature event. This means a file or group of files has a 1-1 relationship between the certificate and the signing event during which the file is submitted for signing.

Keys are never at risk of compromise as they are used only once and if revocation is required no other applications are impacted. It is the safest signing method.

This model is used for Java signing.

#2: On-Demand Keys

This can also be referred to as On-Demand Pool model.

Keys are retained in a pool and assigned a friendly name for easy identification.

When you submit an application for signing you can either choose one of the existing certificates, or create a new one.

This model is ideal if you need to sign files for usage in Android Operating Systems (such as applications), since Android expects you to use the same certificate over and over again for each release of an application. You will therefore have a number of signing certificates associated with a signing service.

#3: Pool of Rotating keys

This model Supports Microsoft Smartscreen Filter reputation model.

If you need to sign files for usage in Microsoft Operating Systems (DLL files, EXE files etc.) then Microsoft expects you to cycle through a pool of certificates rather than using the same certificates over and over again for signing.

Keys are generated on demand as needed, and must be unique across a set number of days (1, 8 or 15). Once the number of days is reached, the keys are then re-used.

Microsoft gives higher levels of repudiation to publishers using this model. As a result we implement this for all our Microsoft based signing services.

Which signing model do I need?

The models to use depend on the signing service requested but also on your own requirements/policies. For example, the *on-demand* signing model is often used for Android apps, but it can be used for several other signing services as well.

If you are looking for a “default” option, here is what we would recommend:

- Java files: unique keys
- Android files: on-demand keys
- Microsoft files: rotating keys
- Other files (default): unique keys

All signing models are enabled by default on SAS. When you select a signing service (e.g. Authenticode signing) the platform will automatically select the relevant model for you (the pool of rotating keys in this instance). It is possible to change this automatic selection for the signing service of your choice to align with your needs and maximise security.

Lightning-fast application signing on Windows, OpenSSL and Java

Symantec Secure App Service enables you to sign large-sized applications without uploading them to the Secure App Service cloud.

The solution works in partnership with our APIs and a local application installed to perform signing of large files by computing the hash of the application being requested for signing and passing that hash to SAS for signing in the cloud.

Once the hash is signed, SAS sends it back to the local application, which adds it to the local file and thus the application is signed.

You retain the benefit of key protection, user management and reporting provided by SAS.

The malware scanning service included SAS is not available with lightning-fast signing since only the hash of your file is uploaded to SAS, and not the entire file.

Related services

Symantec Secure App Service (SAS)¹ is part of our Complete Website Security (CWS) solution².

¹ <https://www.symantec.com/code-signing/secure-app-service/>

² <https://www.symantec.com/complete-website-security/>