digicert

Hash Signing for Microsoft Windows

Enabling lightning-fast code signing with DigiCert Secure App Service (SAS)

DigiCert Secure App Service (SAS) offers a signing service which enables you to sign files of any size in record times on Microsoft Windows environments. The service works through the deployment of our local CSP (Cryptographic Service Provider) on a computer or into a build environment.

Main benefits:

A lightweight app **+** not much processing **+** the possibility to integrate commands with your own environments / development processes **=** the flexibility you need, and a lot of time saved!

Features

Rather than uploading files to the cloud for signing, our CSP computes the application hash and sends this to the cloud for signing.

- Fully integrated with SAS APIs
- CSP can also be called via Signtool on a command prompt
- Unsigned software never leaves your organisation
- Hours saved: signing a 1.95GB file with a 5MB/s speed will take approximately 24 seconds
- Works extremely well with large files

Components required

SAS CSP: must be installed on the computer where you want to sign your applications (32-bit or 64-bit version available).

Microsoft SignTool: must be available on the computer where you want to sign your applications[1].

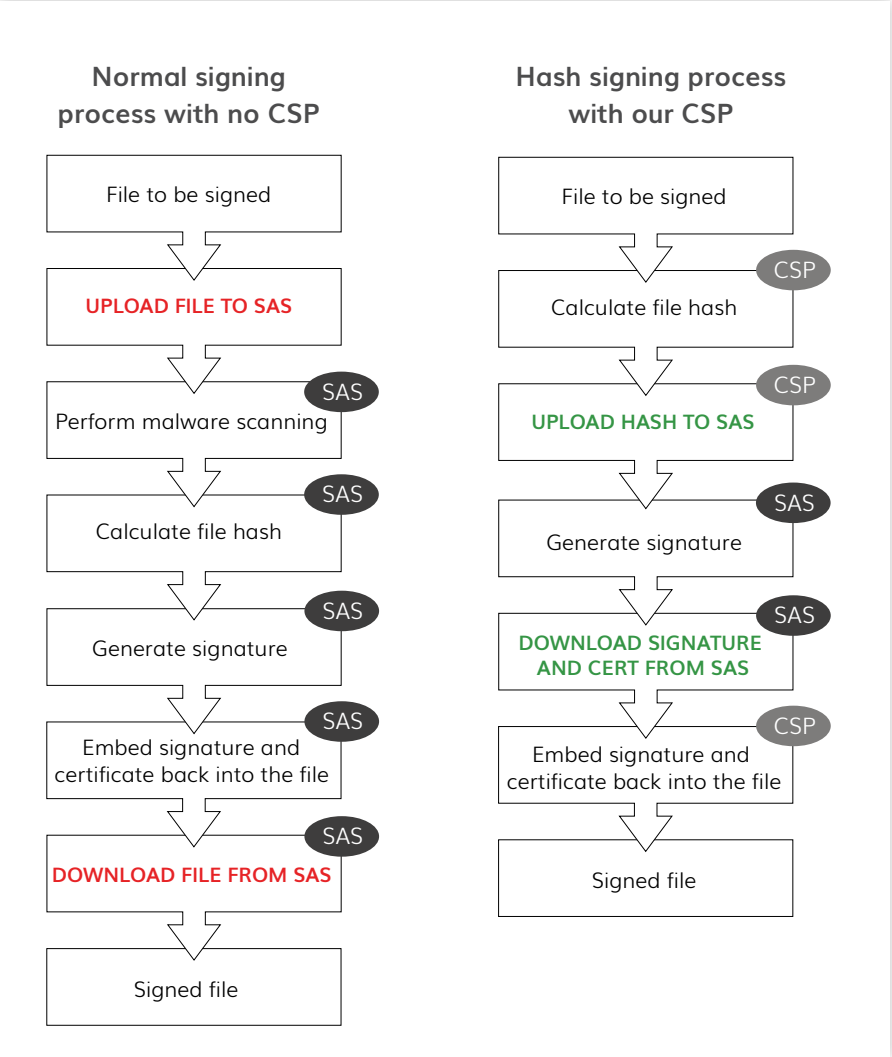
Related services

DigiCert Secure App Service (SAS)[2] is part of our Complete Website Security (CWS) solution[3].

The CSP works in partnership with our APIs and the local Microsoft Windows ***Signtool*** to perform signing of large files by generating the hash of the application being requested for signed and passing that hash to SAS for signing in the cloud. Once signing is completed, the CSP gives the signature back to signtool which then integrates it with the unsigned file to get the signed content.

With hash signing, you retain the benefit of key protection, user management and reporting which SAS provides.

Note that the malware scanning feature which is integrated to SAS (see step 3 of normal signing process) cannot be performed when choosing the hash signing process as only the hash is submitted for signing to the SAS cloud.



[1] https://msdn.microsoft.com/en-us/library/windows/desktop/aa387764(v=vs.85).aspx
[2] https://www.websecurity.symantec.com/complete-website-security
[3] https://www.websecurity.symantec.com/code-signing/secure-app

For more information, contact an IoT expert
1.801.701.9695 or iot@digicert.com

Lehi

2801 North Thanksgiving Way Suite 500
Lehi, UT 84043
USA

Mountain View

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

UK

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

Switzerland

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

Cape Town

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

Australia

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

China

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

Japan

Ginza 3-Chome
5F Okura Bekkan
3-4-1 Ginza Chuo-ku
Tokyo 104-0061
Japan

India

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

digicert® | Symantec™ Website Security