digicert®

Traditional Code Signing Threat Landscape

5 critical vulnerabilities / bad practices to address

Code signing essentially relies on a Public Key Infrastructure, which means code signing certificates are made out of a pair of public and private key - the public key is signed by a trusted Certification Authority such as DigiCert, and the private key is kept by the owner and used to sign the code to secure.

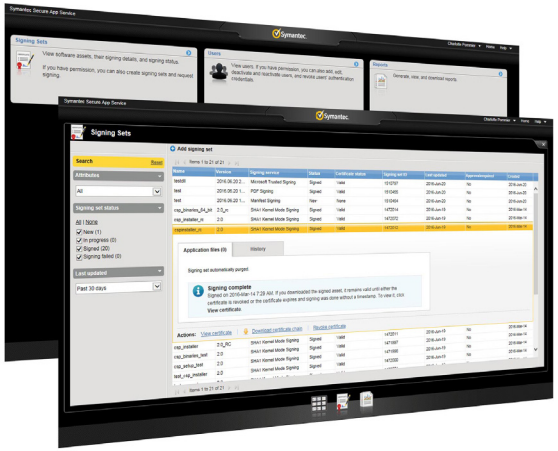
Although the technology behind Code Signing certificates is proven, managing them - and by extension managing the private keys - is an activity that can be very complex, especially when the key owner(s) do not understand their value.

The risks of casual code signing practices to an enterprise can be summarised as follows:

Signing keys are vulnerable to theft	Unless protected correctly, code signing keys can fall into the hands of bad actors. This can lead to malware being signed by your organisation's certificate leading to reputation damage or loss of information.
A single key is used to sign all applications	Each code signing certificate has a unique private key which is used for signing. Unless companies purchase expensive Hardware Security Modules (HSMs) and or purchase multiple certificates then they take a very important risk when they distribute copies of the private key within their organisation.
No accountability for signing and no rights management	Anyone with a copy of the signing keys could sign code and you would not be aware of it. If something goes wrong with your software, you may not know who signed it. You cannot choose who can sign what and it is hard to control and monitor signing delegations if you hire temporary workers or if someone leaves.
No tracking of signing activity or auditing	Some organisations sign thousands of applications per month. Tracking and reporting can quickly become a challenge and you only realise it when it's too late: suddenly Malware is discovered in one of your programmes and you need to know which key was used in order to revoke it. You then also need to know which other programmes were signed by this key.
Spiralling costs of in-house code signing process	Implementing a centralised, bespoke code signing management system is expensive and time-consuming. You will need to purchase multiple code signing certificates and hardware such as HSMs to protect your keys. You will need expertise and skills specific to code signing in order to design and keep this process secure. Finally you will need personnel to manage, maintain and grow your process as and when your code signing needs to evolve.

How can DigiCert help?

In order to help customers to solve for the shortcomings in regard to the management of code signing private keys and user access, DigiCert has developed **Secure App Service**. Secure App Service is a cloud-based code signing key protection and management service which looks to address all of the core risks associated with code signing and more.



The Secure App Service platform

The concept is simple yet very effective: instead of being issued and used locally, certificates are directly issued and stored in a secured cloud, where files are submitted for signing, and sent back to the user once signed.

This system not only solves all these key signing management risks but also offers extra protection and features for all your code signing needs.

What you can expect from Secure App Service as a mature cloud-signing service:

What you can expect from Secure App Service as a mature cloud-signing service:

- **Your signing keys will never be compromised** - Keys are stored in a military grade data center and backed by leading industry certifications: WebTrust, KPMG audits, SAS 70, CA/Browser Forum. NetSure insurance coverage of $1.5M for proper certificate issuance and compliance with CP/CPS.
- **You will meet compliance requirements** - Embedded time-stamping, support for multiple signing types, unique keys where possible, 3rd-party Test House support, and full reporting and auditing of activity.
- **You have a quick mitigation solution when things go wrong** - Admins can revoke any certificate as necessary. DigiCert will provide "white glove" treatment for backdating revocations in order to limit loss of previously signed apps.
- **Your access to SAS will not be compromised** - Each user can be assigned specific roles and placed in Work Groups. The access to SAS is granted thanks to client certificates for authentication. We offer optional approval queue, two factor authentication and IP whitelisting to ensure only IP addresses from your organisation are permitted.
- **You will benefit from a subscription pricing model** - SAS offers a fixed price based on the number of signing events an organisation will perform in a year. There are no hidden charges for creating certificates and no requirement to purchase or maintain hardware on behalf of the organisation.

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