Safeguard Business and IoT Integrity Symantec Secure App Service: Unrivaled code signing service and security for IoT

The Internet of Things (IoT) has rapidly transformed the digital landscape and the world we live in. Intelligent devices and sensors connect smart cars, robotic manufacturing equipment, smart medical equipment, smart cities, industrial control systems, and much more in a way that improves lives and saves businesses billions of dollars. But along with its benefits, rapid IoT growth introduces a new dimension of security vulnerabilities that dramatically escalates the nature and seriousness of cybercrime risks.

In addition to traditional confidentiality cyber risks, IoT threats include attacks that can:

- Render smart appliances useless.
- Shut down city power grids.
- Threaten lives through hacked pacemakers and other medical devices.
- Create costly and deadly industrial accidents and hazards.
- Stall the entire Internet with bot infected surveillance cameras.
- Hijack the acceleration, steering, and brakes of smart cars.

Such security flaws not only endanger lives, frustrate customers, and disrupt business operations, but they create significant cost and public relations damage for IoT developers and manufacturers. A prime example of this is the recent 1.4 million auto recall of a car model that had a flaw that let attackers remotely take over its operations.

The biggest factor at the heart of all of these risks is that software can be tampered with too easily unless protected by code signing. That's why code signing of IoT device software has become imperative. No IoT device should run unsigned code. It's simply too dangerous to accept data from unverified devices or unverified services.

Code signing all your IoT firmware and software gives you greater control in keeping malware authors from injecting malicious code into your devices. It acts as digital shrink wrap around your software and updates, confirming that it comes from a verified source and that it hasn't been tampered with since the moment it's been signed. It also gives you the ability to only allow code signed by a specific authority to run on your firmware. In other words, you can become your own code signing authority for your IoT devices and you can make sure that your firmware only accepts code signed by you.

To help you protect your business against major financial loss and brand damage, Symantec Secure App Service secures and simplifies IoT code signing with the visibility, agility, and security you need from the global cyber security leader you can trust.

Protect your IoT device and business integrity.
Code signing can help you make sure your IoT devices:

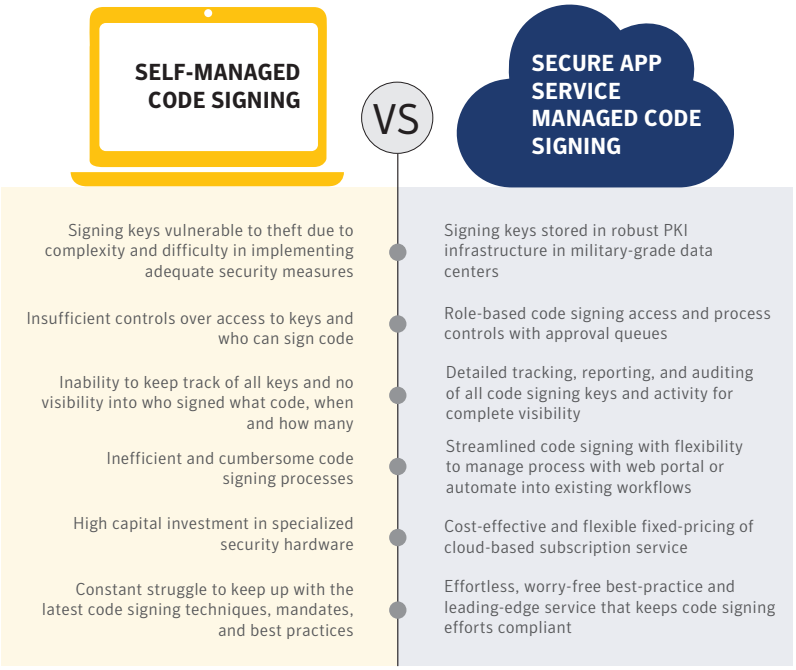
- Only accept code from reliable sources
- Only run signed and validated code
- Only do what you program them to do

Secure keys with fast and simple code signing.
To make sure cybercriminals can't tamper with the software embedded in your IoT devices you have to do more than just code sign. You have to keep your private code signing keys safe. Code signing consists of digitally signing your software with a digital certificate issued by a certificate authority (CA). The security of these certificates relies on a pair of keys—one public and one private. If someone steals your private keys, they can use it to sign malware and legitimately distribute it to all your IoT devices.

Failure to protect your keys opens the door for cybercriminals to take complete control over your IoT solutions. Secure App Service gives you the depth and breadth of protection you need to secure your keys, while taking the effort and worry out of code signing your IoT software.

Instead of trying to manage your own IoT code signing efforts, Secure App Service simplifies and secures your IoT code signing by making the process easy.

- Upload your software or file hash to our secure cloud service and we sign it for you.
- Use our management dashboard or tie the service into your custom build processes with our APIs.
- Trust us to securely store your certificates and keys in the cloud in our highly secure data center.
- No longer worry about the security risks, management complexity, and hardware security investments associated with storing keys locally.



Full-scale IoT security.

In addition to protecting the integrity of the software in your IoT devices with code signing, Symantec offers other solutions that add different layers of security to give you even more comprehensive IoT protection:

- Strong mutual authentication for user-to-device, services- to-device, and device-to-device communications
- Powerful, chip-efficient encryption to protect over-the-air data communication and dataat- rest
- Host-based protection and hardening to mitigate advanced threats
- Dynamic IoT security management

Secure IoT software with flexible code signing options.
The highly innovative, expansive, and constantly changing nature of IoT can lead to very diverse development environments that need to support a wide variety of software file types. To support the diverse nature of IoT software, we offer code signing flexibility with support for OpenSSL, GPG, and RPM. Each of these signing types include the ability to sign IoT firmware and OS images, as well as small to large file sizes and different flavors of software.

IoT code signing options with Secure App Service	Open SSL	GPG	RPM
Key models	Fixed cert pool (On-demand) Unique key model	New key Fixed cert pool	New key Fixed cert pool
File types	All	All	.rpm
Full file upload only versus hash-based signing	Hash-based and full file upload	Full file upload only	Full file upload only
Digest algorithms	SHA1 SHA256	SHA1 SHA256	SHA1 SHA256
Signing options	RSAUT DGST	sign (binary) clearsign detach-sign	addsign resign

Gain complete control over and insight into all IoT code signing activity to protect your business and IoT integrity. Backed by one of the global cyber security leaders, Symantec Secure App Service helps protect your business against major financial losses and brand damage with simplified, no-worry IoT code signing visibility, agility, and security.

Complete Website Security:

Backed by one of the global leaders in cyber security, Symantec Complete Website Security harmonizes and fortifies your website security with visibility, agility, and best-in-class security to protect your business, brand, and customers with confidence.

Contact us:

For product information in the UK, call:
0800 032 2101 or +44 (0) 203 788 7741
Symantec (UK) Limited.
350 Brook Drive,
Green Park, Reading,
Berkshire, RG2 6UH, UK.
www.symantec.com/en/uk/complete-website-security

For product information in Europe, call:
+353 1 793 9053 or +41 (0) 26 429 7929

For product information in the US, call:
1-866-893-6565
Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/complete-website-security

For product information in Asia Pacific, call:
Australia: +61 3 9674 5500
New Zealand: +64 9 9127 201
Singapore: +65 6622 1638
Hong Kong: +852 30 114 683

Symantec Website Security Solutions Pty Ltd
3/437 St Kilda Road, Melbourne,
3004, ABN: 88 088 021 603
www.symantec.com/en/aa/complete-website-security