Safeguard Business and IoT Integrity with 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.

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

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.

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.

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.

Full-scale IoT security

In addition to protecting the integrity of the software in your IoT devices with code signing, DigiCert 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 data-at-rest
- Host-based protection and hardening to mitigate advanced threats
- Dynamic IoT security management

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.

SELF-MANAGED CODE SIGNING

VS

SECURE APP SERVICE MANAGED CODE SIGNING

Signing keys vulnerable to theft due to complexity and difficulty in implementing adequate security measures	Signing keys stored in robust PKI infrastructure in military-grade data centers
Insufficient controls over access tokeys and who can sign code	Role-based code signing access and process controls with approval queues
Inability to keep track of all keys and no visibility into who signed what code, when and how many	Detailed tracking, reporting, and auditing of all code signing keys and activity for complete visibility
Inefficient and cumbersome code signing processes	Streamlined code signing with flexibility to manage process with web portal or automate into existing workflows
High capital investment in specialized security hardware	Cost-effective and flexible fixed-pricing of cloud-based subscription service
Constant struggle to keep up with the latest code signing techniques, mandates, and best practices	Effortless, worry-free best-practice and leading-edge service that keeps code signing efforts compliant

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 flavorsof 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, our Secure App Service solution helps protect your business against major financial losses and brand damage with simplified, no-worry IoT code signing visibility, agility,and security.

About us

DigiCert is the world's premier provider of high-assurance digital certificates. Since our founding almost fifteen years ago, we've been driven by the idea of finding a better way. A better way to provide authentication on the internet.

A better way to tailor solutions to our customer's needs in SSL, PKI and IoT security. Now, we've added Symantec's experience and talent to our legacy of innovation to find a better way to lead the industry forward and build even greater trust in the world's digital interactions.

For more information call + 44 (0) 208 528 1415, email enterprise@digicert.com or visit digicert.com/contact-us

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