Secure Code Signing and Update Delivery for the Internet of Things (IoT)

Venafi Next-Gen Code Signing and Device Authority KeyScaler

Introduction

What is code signing?

Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been changed or corrupted since it was signed. The process uses a cryptographic signature/fingerprint to validate authenticity and integrity of the delivered software.

Why is code signing important for update delivery?

IoT devices are usually updated automatically without direct end user intervention. Because of this, software updates can be a key target for cybercriminals to add malicious code. These updates could be used to gather sensitive customer information and/or change the operating behavior of the device damaging the IoT vendors reputation. Without code signing, the IoT device vendor cannot guarantee that delivered updates isn't modified by third parties.

The Challenge for IoT

Connected/IoT devices are only as valuable as the operating systems and applications that they execute. The firmware, operating system and application update processes are highly sensitive and can be a prime target for attack. Hackers have used these methods and systems from Microsoft, ASUS, and others to spread malware that is completely 'trusted' and can avoid Next-Generation Antivirus (NGAV).

Establishing control over all assembly, authorization, signing, and distribution processes can significantly reduce the risk of successful attack and solve some very important problems including:

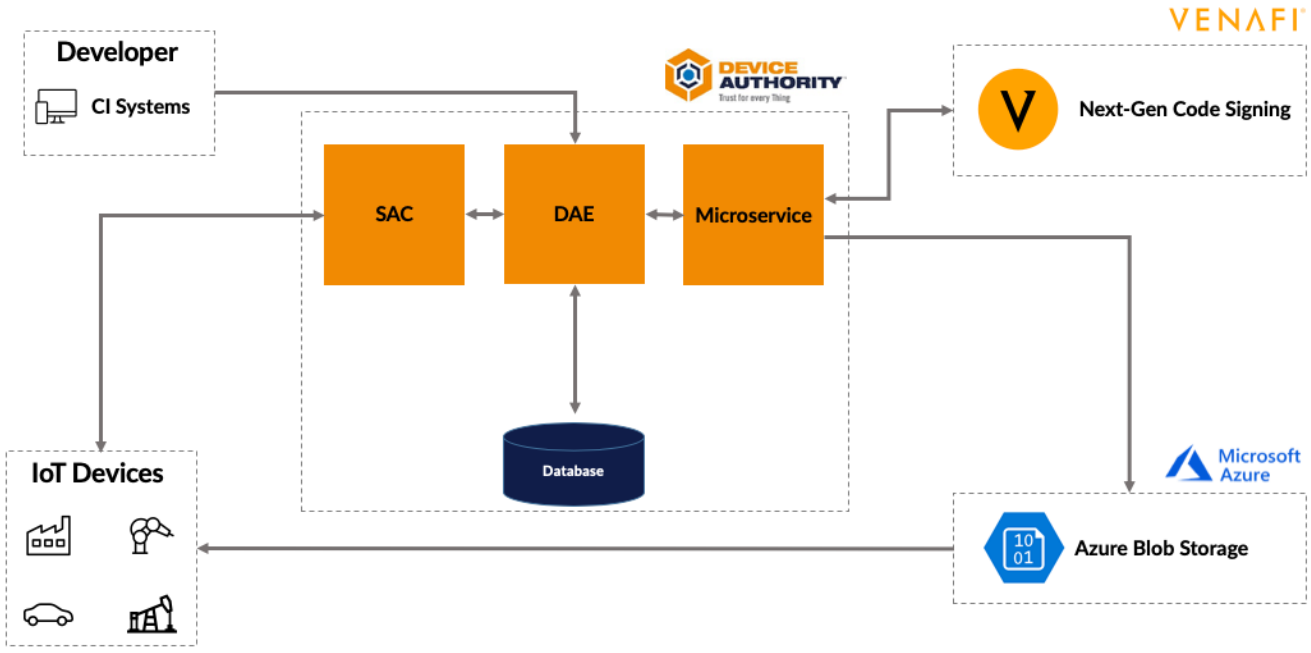
- Organizations need a method to trust and verify IoT device updates
- Unverified device updates are easy entry point for attackers
- Unsigned updates can be tampered in transit
- Need to be able to prevent malicious updates being applied to devices
- No integration with existing enterprise systems

- Existing code signing solutions are not integrated with IoT workflows
- Existing IoT code delivery processes not readily integrated with code-signing workflows
- Even if code signing is currently being used for software updates, the process by which the code signing keys are used is not adequately protected making them vulnerable to theft and/or misuse
- Software development and delivery teams may not have the PKI expertise necessary to properly utilize code signing to protect delivered software
- New solutions are built from scratch for each use-case

The process of update build, code signing (if performed), and distribution are disparate functions without end-to-end control, visibility, and auditing. This leaves many possible gaps open to exploit causing a cascading impact that enables adversaries. In the case of IoT, there needs to be trust association with the edge/device and the process has to be managed without human intervention. This provides adversaries with essentially a cyberweapon with huge breadth, high success, and immensely damaging impact.

Our Solution: Turnkey Secure Code Signing and Update Delivery

Device Authority's KeyScaler platform provides an automated solution to manage the lifecycle of updates that are delivered to a device. Provisioning unique certificates, establishing trust between a device and server, signing code using a pre-configured Certificate Authority with policy-based authorization, and delivering encrypted assets to IoT devices – without requiring any human intervention. This solution closes the gaps open to exploitation by integrating and using Venafi Next-Gen Code Signing to secure the code signing process throughout the secure update lifecycle.



How does it work?

The end-to-end solution is broken down in to two distinct processes:

1. Code Signing

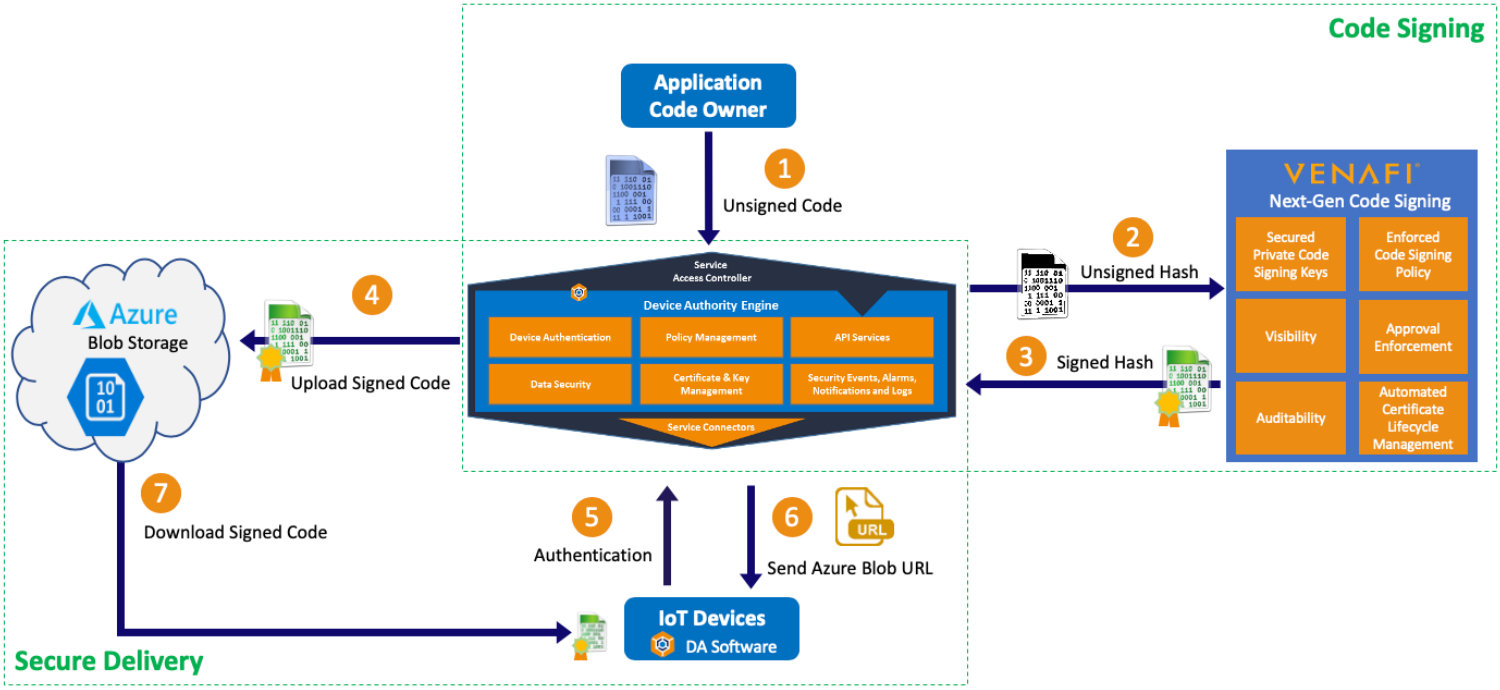
This process is responsible for taking the unsigned data, submitted to KeyScaler through the REST API, and utilizing the Venafi Next-Gen Code Signing solution to cryptographically sign the data, using the appropriate code signing certificate. Venafi Next-Gen Code Signing ensures that the secured code signing private keys never have to leave their protected location and that any predefined approval workflows needed for accessing the code private signing keys are enforced. Software developers continue to use the native code signing tool that they normally do. This tool will generate a hash, the hash is automatically sent to Next-Gen Code Signing which then signs it with a private key and then returns the signed hash. The code signing tool then adds the signed hash to the software application to create a signed application.

The InfoSec team establishes baseline requirements for code signing (e.g. which certificate authority to use, encryption strength, etc). Application teams define the approvals that are required before an application can be signed along with the tools, machines, and people that are authorized to sign the application.

The application team uses the native code signing tool that comes with their development environment to sign code as they normally do. However, when this tool is invoked, it sends the hash of the application to Venafi Next-Gen Code Signing instead of sending the complete application. This significantly improves the speed by which the application is signed. Next-Gen Code Signing automatically enforces any policies that are put in place such as which keys are available for use, who is required to approve the signing operation, and what types of applications can be signed with the key. The signed hash is returned to the code signing tool which then completes the code signing operation.

2. Update Delivery

Once the code has been signed, it must be delivered to the KeyScaler-managed devices. The update delivery process is responsible for uploading the signed update to a repository, and providing the download URL to the appropriate devices upon next check-in.



KeyScaler Update Policies

In addition to the Venafi code signing policies, KeyScaler will provide update policies that define how the code signing and update delivery functions behave – as well as defining what happens if the device does not apply the update within the configured time period.

Venafi Next-Gen Code Signing

Venafi Next-Gen Code Signing is built on top of the Venafi Platform which protects machine identities by orchestrating cryptographic keys and digital certificates for SSL/TLS, IoT, mobile, code signing, and SSH for the extended enterprise—on-premises, mobile, virtual, cloud, and IoT—at machine speed and scale. Venafi automates the entire key and certificate life cycle as well as remediation to reduce or eliminate security and availability risks connected with weak certificates (such as SHA-1, MD5 or wildcard certificates) or compromised machine identities.

Venafi Next-Gen Code Signing not only secures private code signing keys but also secures the process by enforcing industry-accepted best practices. Together, these solutions secure the storage of private code signing keys, automate code signing policy enforcement, manage the full lifecycle of code signing certificates, separate code signing roles and responsibilities, and provide a full audit trail of code signing activities.

Venafi Next-Gen Code Signing automates the full certificate lifecycle in addition to enforcing and

automating a secure code signing process. Software developers continue to use the code signing tools that they have always used. Private code signing keys always remain protected within the Venafi secure storage, or a connected Hardware Security Module (HSM). Access to these keys is controlled by the code signing process enforcement policies that have been defined in the Venafi platform.

Device Authority Code Signing and Secure Updates

Device Authority Code Signing and Secure Updates solution delivers each of these critical requirements for IoT environments:

- Access to secure updates is restricted to authorized devices
- Updates are also specifically encrypted for target devices and are not exposed as unprotected software or firmware downloads
- Secure updates ensure that both the update source and the integrity of the updates themselves are verified, delivering end-to-end protection for device updates

Delivering Secure Code Signing and Update Delivery for IoT

Together, Venafi Next-Gen Code Signing and Device Authority KeyScaler integrate seamlessly to secure your code signing and update delivery process for IoT devices.

This provides value to organizations in many industries by delivering:

- Automated code signing certificate lifecycle which eliminates the requirement for software teams to manage this themselves
- Secure code signing and update delivery activities through policy enforcement
- Trusted and validated IoT device updates

Interested in Learning More? Contact Us!

www.deviceauthority.com

info@deviceauthority.com

About Venafi

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe encryption, authentication, and authorization. Organizations use Venafi key and certificate security to deliver safe machine-to-machine connections and communications—protecting commerce, critical systems and data, and mobile and user access.

About Device Authority

Device Authority is a global leader in Identity and Access Management (IAM) for the Internet of Things (IoT); focused on medical / healthcare, industrial and smart connected devices. Our KeyScaler™ platform provides trust for IoT devices and the IoT ecosystem, to address the challenges of securing the Internet of Things. KeyScaler uses breakthrough technology including Dynamic Device Key Generation (DDKG) and PKI Signature+ that delivers unrivalled simplicity and trust to IoT devices. This solution delivers automated device provisioning, authentication, credential management and policy based end-to-end data security/ encryption.

With offices in California, US and Reading, UK, Device Authority partners with the leading IoT ecosystem providers, including AWS, DigiCert, Gemalto, HID Global, Intel, Microsoft, nCipher Security, PTC and Thales. Keep updated by visiting www.deviceauthority.com, following us on Twitter @DeviceAuthority and subscribing to our BrightTALK channel.

sales@deviceauthority.com
www.deviceauthority.com

DEVICE AUTHORITY™