BlackBerry | certicom

BlackBerry Certicom Code Signing and Key Management Server:

Quantum Resistant Code Signing for Software Protection

Quantum Computing Threat

Quantum computing promises to solve groundbreaking problems in particle physics, pharmaceuticals, healthcare, logistics and many other fields. Despite the benefits, it may also give cybercriminals or nation-state sponsored hackers the ability to crack traditional public key cryptosystems and subvert these systems at their foundation.

Such an attack is a real concern for systems which need to be deployed for several years or even decades of operation – and thus present an opportunity for malevolent actors.

Certicom has the solution – by adding our robust quantum-resistant code signing server to your cybersecurity defenses, you can address this latent security threat.

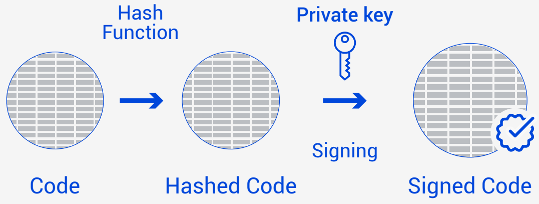
Code Signing

Code signing is the process of applying a digital signature to device firmware or application software. It employs cryptographic algorithms to create high-assurance seals which can be used to authenticate that the software was created by a trusted party has not been tampered with. If you don't sign your code, anyone can replace it with malware.

Traditional code signing uses RSA or ECDSA-based key pairs to sign and verify software. Quantum resistant code signing uses algorithms that are resistant to quantum computer-based attacks and thus secures long-lived devices and applications for a future when such attacks may be likely.

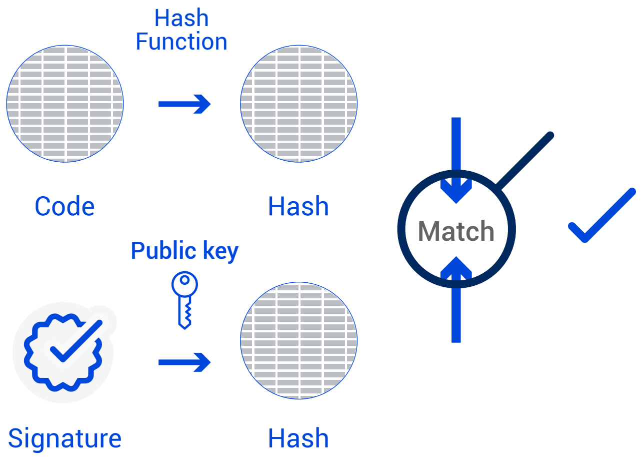
How Code Signing Works

Code Signing Mechanism



Application developers and software publishers use code signing to attach a unique digital signature or seal to firmware or application software as a way to ensure authenticity and integrity. Operating systems, software applications and devices verify a trusted digital signature to authenticate the source of the code and confirm that it has not been altered.

Code Verification Mechanism



Signing Application vs Secure Signing Server

Even if quantum attack is not an immediate concern, and you are using traditional RSA or ECDSA signatures for code signing, if you are not using robust security and access control mechanisms to protect code signing keys, there is a good chance that your organization isn't using best practices to protect your products.

The abuse of code signing schemes is widely known – StuxNet is an infamous example where signing keys were stolen and signed malware used to mount cyberattacks. Code signing keys need to be well protected. This is particularly vital to securing software deployed in critical infrastructure and safety-critical devices which will be in use for many years into the future. Certicom's hardened code signing server mitigates these risks by protecting code signing keys and access to them. Employing an HSM for signing key operations, it provides robust security for the control and administration of code signing and optional encryption keys for protecting device firmware and software applications.

The Solution: Certicom Code Signing and Key Management Server

The code signing key server supports quantum-resistant hash-based HSS and XMSS digital signatures as well as traditional RSA and ECDSA-based signatures to secure software images.

Code signing and encryption functionality can sign a pre-computed hash or compute and sign a hash from a presented file image, logging the resulting signature and metadata.

Digital signatures created with quantum resistant signatures will protect firmware and software images in long-lived assets against a future when quantum computers will be able to crack traditional code signing schemes.

Critical to the security of code signing solutions is the protection of private keys in traditional signature schemes and the protection of key states in one-time signature algorithms such as HSS and XMSS.

The key management server (KMS) also supports AES management, offering key derivation options for file encryption and key wrapping to support firmware encryption and MAC based image authentication.

Features:

- Traditional RSA, ECDSA & Quantum Resistant HSS & XMSS digital signatures
- RESTful API for easy integration with code signing clients
- Secure logging of meta data associated with signed images
- Administration of signing keys using project and user permissions
- FIPS 140-2 certified hardware security modules to protect sensitive keying material
- Signing and encryption of block images or simple signing of presented hash fingerprints

Specifications:

Cryptographic algorithm support

- RSA, ECDSA and HSS and XMSS hash-based signatures
- AES encryption, HMAC-KDF, CMAC
- RSAES-OAEP and PKCS #11 key wrapping

Key Administration and Protection

- M-of-N based hardware tokens for key administration & control
- Keys managed on a project basis
- Keys protected in a FIPS 140-2 Level 3 (physical) HSM

Powerful, reliable platform

- 2.1 GHz Intel Xeon Silver 4110 processor, 8 cores

Storage

- High performance, RAID 1 storage subsystem with SSD drives

Enclosure

- 2U rack mounted server
- 3.5" hot-swap drive bays
- Redundant hot-swap (100 - 240 V) high efficiency power supplies

Network Interface

- 2x Integrated 1 GbE RJ-45 ports
- 1x RJ-45 10/100/1000 Mb Ethernet systems management port

Secure Operating Environment

- CentOS 7 based hardened SE Linux platform

Benefits of Certicom's Code Signing Key Server

1. **Security of Signing keys:** Reduce risk of key leakage, theft or misuse via containment in a hardened signing server. This reduces the risk of keys been lost or stolen and tampered with.

2. **Ease of Control:** The code signing key server provides a centralized signing solution which offers better administration and visibility of signing operations for authorized users and client applications.

3. **Cost-effectiveness:** The code signing key server is a turnkey solution with easy to use APIs which allow robust code signing practices to be easily integrated into software development and release processes across the enterprise.

4. **Increased Policy and Audit Compliance:** Using Certicom code signing key server provides a secure audit trail of individuals or applications who used protected keys to sign or encrypt code, supporting corporate security policies and security best practices.

Why BlackBerry Certicom?

- Market leader in Key Management Platforms
  - Expertise in applied cryptography with decades of experience in a variety of markets
- Part of the Trusted Blackberry Brand
  - Certicom is a critical component of the Blackberry group with a focus on cybersecurity. With over 30 years of experience in applied cryptography, Certicom has distinguished itself through outstanding innovations demonstrated through the acquisition of numerous patents and award-winning software
- Long-Term Commitment to Customer Base
  - By supporting several distinct security solutions in long-term customer deployments, Certicom has demonstrated its understanding and commitment to support products in the field despite constant changes to core computing technology

BlackBerry | certicom

Certicom Corp., subsidiary of BlackBerry manages and protects the value of content, applications, and devices with government-approved security. Elliptic Curve Cryptography (ECC) provides the most security-per-bit of any known public key scheme. As the global leader in ECC, Certicom has licensed its security offerings to hundreds of multinational technology companies, including IBM, General Dynamics, and SAP. Founded in 1985, Certicom's corporate office is located in Mississauga, Ontario, Canada.

www.certicom.com