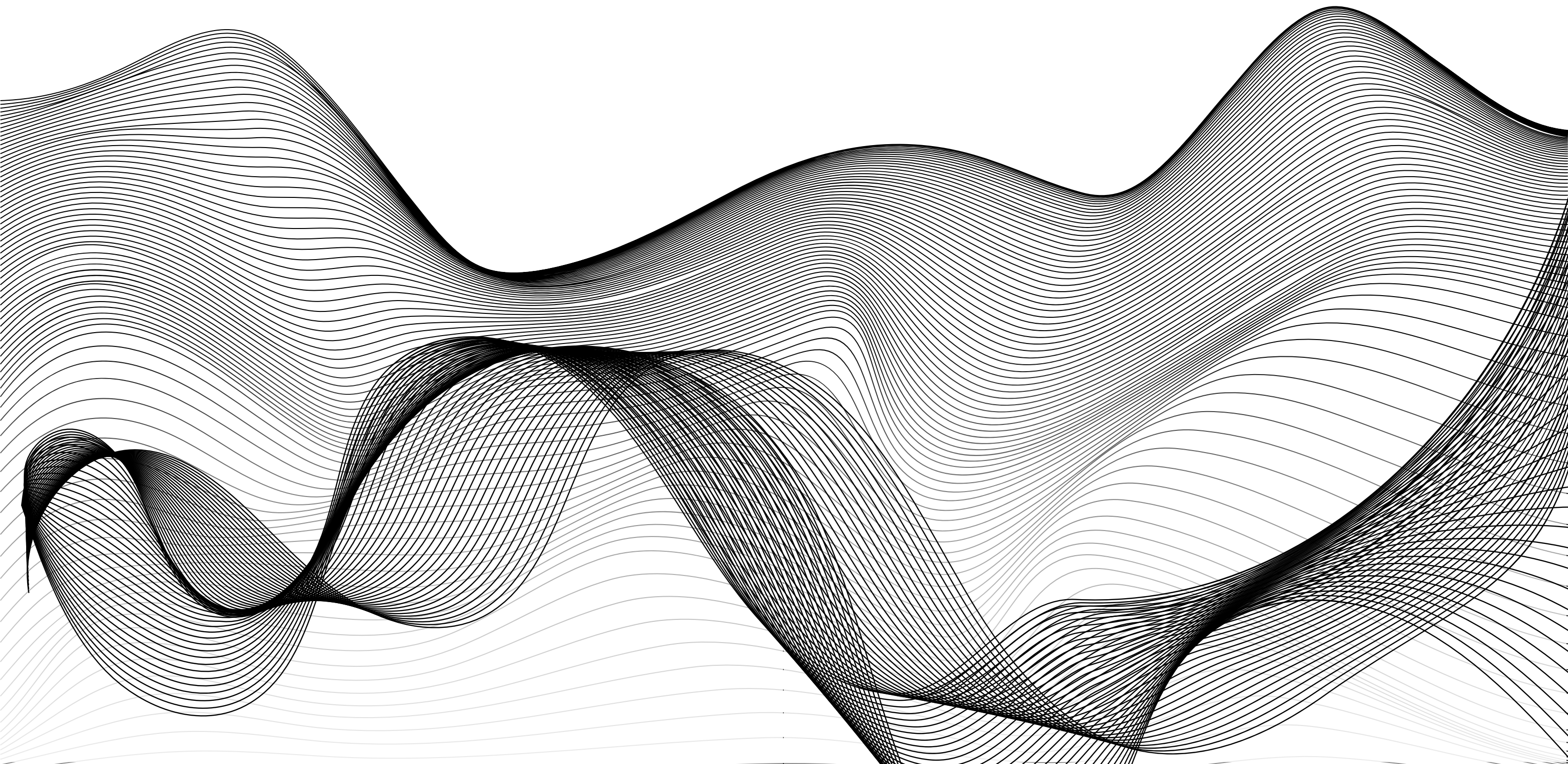
Securing Your Code Signing Keys with Fortanix and SSL.com: A Comprehensive Solution

An SSL.com White Paper

May 2024



Introduction

Code signing has become essential for software developers to establish trust and integrity of their applications. However, managing code signing keys and obtaining trusted certificates can be challenging, especially considering the stringent requirements for key storage and the complexities of integrating with automated CI/CD pipelines. This white paper explores the partnership between Fortanix and SSL.com, which offers a comprehensive solution to address these challenges and streamline the code signing process.

Requirements and Challenges

Storage Requirements for Code Signing Certificate Key Material

One of the primary challenges in code signing is ensuring the compliant storage of private key material that is bound to a code signing certificate. . Microsoft, for example, requires that code signing keys be generated and stored on a compliant hardware security module (HSM) device. Additionally, proof must be provided that the keys were generated on a compliant HSM in a complaint manner and are stored in a complaint way. This proof is referred to as an “attestation” as the entity managing the HSM and the key material are attesting to the fact that the key storage meets those compliance standards. Integrating this key material into an automated CI/CD pipeline can be a complex task, adding further complications to the process.

Limitations of Physical Networked HSMs

Traditional physical networked HSMs come with their own set of challenges. These devices are expensive to acquire and maintain, requiring dedicated infrastructure and expertise. Scaling the code signing process with physical HSMs can be cumbersome and integrating them seamlessly into modern development workflows can be daunting.

Obtaining a Publicly Trusted Certificate

To establish trust with end-users, obtaining a code signing certificate from a publicly trusted Certificate Authority (CA) is crucial. However, navigating the validation process and selecting the appropriate type of certificate (OV or EV) can be confusing for developers who are not well-versed in the intricacies of PKI.

What You Need to Know to Solve the Problem

Understanding Certificate Authorities and Identity Validation

A Certificate Authority (CA) is a trusted entity that issues digital certificates to validate the identity of individuals, organizations, or devices. In the context of code signing, a CA verifies the software publisher's identity and issues a code signing certificate that attests to this identity. Understanding a CA's role and the importance of identity validation is crucial for obtaining a trusted code signing certificate.

Choosing the Right Type of Code Signing Certificate

Two main types of code signing certificates exist: Organization Validation (OV) and Extended Validation (EV). OV certificates provide a basic level of assurance about the publisher's identity, while EV certificates involve a more rigorous validation process and offer the highest level of assurance. Selecting the appropriate type of certificate depends on the specific requirements of the software distribution platform and the level of trust desired.

Microsoft-Trusted Code Signing Certificates

It is essential to obtain a Microsoft-trusted code signing certificate to distribute software through Microsoft's platforms, such as Windows or the Microsoft Store. CAs that have met Microsoft's strict requirements for identity validation and critical management practices issue these certificates. A Microsoft-trusted certificate ensures that Microsoft's operating systems and distribution channels will recognize the signed code as trustworthy.

The Importance of Attestation

Attestation proves that the code signing keys were generated and stored on a compliant HSM device. This is a critical requirement for obtaining a Microsoft-trusted code signing certificate. The attestation process typically involves generating a signed statement from the HSM that includes information about the key's origin and the compliance status of the HSM. Without proper attestation, Microsoft or other relying parties may not recognize the code signing certificate as valid.

Benefits of Cloud HSMs over On-Premises HSMs or Tokens

Cloud-based HSMs offer several advantages over traditional on-premises HSMs or hardware tokens. Firstly, cloud HSMs are highly scalable, allowing organizations to expand their code-signing capabilities as their needs increase. Secondly, cloud HSMs eliminate the need for organizations to maintain and manage physical hardware, reducing operational complexity and costs. Cloud HSMs can be seamlessly integrated into automated CI/CD pipelines, enabling developers to sign code as part of their existing development workflows.

Why Choose SSL.com and Fortanix

Fortanix: A Compliant Cloud HSM Service for Microsoft-Trusted Certificates

Fortanix provides a cloud-based HSM solution that meets all the requirements for storing code signing keys bound to Microsoft-trusted code signing certificates. Its HSMs are certified to the highest standards, ensuring that keys generated and stored within it comply with Microsoft's requirements. With Fortanix, organizations can benefit from the scalability and ease of integration offered by a cloud-based HSM without compromising on security or compliance.

SSL.com: Trusted CA with Expert Support

SSL.com is a globally trusted Certificate Authority that offers a wide range of digital certificates, including code-signing certificates. Its team of experts provides extensive support and guidance throughout the identity validation process, ensuring that organizations can obtain the necessary certificates efficiently. By partnering with SSL.com, organizations can rely on a trusted CA to issue their code-signing certificates, establishing a solid foundation of trust with their end-users.

Seamless Integration between Fortanix HSM and SSL.com

The partnership between Fortanix and SSL.com provides a streamlined and automated solution for code signing. Through native integration, organizations can purchase code signing certificates from SSL.com and have them automatically linked to keys generated within the Fortanix HSM. This integration simplifies the attestation process, as the necessary attestations are automatically generated and included in the Certificate Signing Request (CSR). As a result, organizations can obtain a complete code-signing solution from two trusted entities through a single, unified integration.

Conclusion

Code signing is critical to establishing trust and integrity in the software development lifecycle. However, the challenges associated with key management, compliance, and certificate acquisition can be daunting for organizations. The partnership between Fortanix and SSL.com addresses these challenges by providing a comprehensive and streamlined solution for code signing. Fortanix's compliant cloud-based HSM and SSL.com's trusted CA services, organizations can securely store their code signing keys, obtain Microsoft-trusted certificates, and automate the attestation process. This integration simplifies the code signing workflow, enabling developers to focus on building high-quality software while relying on a robust and compliant infrastructure for key management and certificate issuance.

Fortanix and SSL.com partnership offers a turnkey solution for organizations seeking to enhance the security and trust of their code signing process. By combining the strengths of a compliant cloud HSM and a trusted CA, this partnership empowers organizations to navigate the complexities of code signing quickly and confidently.

All rights reserved. This content may not be reproduced or redistributed without the express written permission of SSL.com. Information is provided "as is" without warranty of any kind, no legal advice or other professional assistance is offered. SSL.com does not accept any responsibility for any errors or any consequences arising from the use of this information.

TRUST IS WHAT WE DO.