yubico

carahsoft.


yubico

Protection for cryptographic keys with the world's smallest hardware security module (HSM)

The YubiHSM 2 is available as a FIPS 140-2 validated, Level 3 solution, or as a non-FIPS solution, both with the same capabilities. Both solutions ensure uncompromised cryptographic hardware security for applications, servers and computing devices at a fraction of the cost and size of traditional HSMs.

Cryptographic Keys Stored in Software are Vulnerable to Threats

The cost of global cybercrime expected to be $6 trillion in 2021, an increase from $3 trillion 2015.* Software storage of cryptographic keys for servers is increasingly vulnerable as attacks become more sophisticated. For example, if a private key is compromised from a Certificate Authority (CA), an attacker can pretend to be your website.

The YubiHSM 2 and YubiHSM 2 FIPS Change the Game for Effective Key Security

Ensure secure hardware cryptographic key storage and operations for applications, servers and computing devices while eliminating the cost and complexity of traditional Hardware Security Modules (HSMs. Yubico's HSM solutions are tamper-resistant and offer low cost, high security ROI in a portable "nano" form-factor that allow flexible use across diverse devices and locations. With the YubiHSM 2 and YubiHSM 2 FIPS, organizations can prevent cryptographic keys from being copied by attackers, malware and malicious insiders. Enterprises can rapidly integrate with either HSM option using the open source SDK 2.0.

Secure Hardware Protection for Cryptographic Keys

Cryptographic keys stored in software can be copied, and are vulnerable to accidental distribution and remote theft. Without strict procedures, it is easy for admins or malicious insiders to backup keys to USB flash drives, FTP them, or share to others via a cloud storage service. Additionally, sophisticated attackers can gain admin access or deploy trojan malware that installs on servers, searches for cryptographic keys, and then copies them for sale on dark web sites like Alphabay.

*Cybersecurity Ventures

Securing the Cryptographic Key Lifecycle

The hardware-based HSM solutions enable secure key storage and operations by preventing accidental copying and distribution of keys, and by preventing remote theft of keys stored.

- Secure key storage and operations on tamper-resistant hardware, with audit logging.
- Extensive cryptographic capabilities including hashing, key wrapping, asymmetric signing, decryption, attestation and more.

Innovative Design for Flexible Use

Traditional rack mounted and card based HSMs are not practical for many organizations because of issues accommodating the HSM's size and deployment complexity. Additionally, rack space at shared data centers often includes physical server enclosures with metal mesh doors to secure access restricting available space.

With Yubico's HSM solutions organizations can easily secure servers, applications, databases, assembly lines, IoT devices, cryptocurrency exchanges and more with a portable "nano" form factor that allows fast and flexible deployment across diverse environments.

The YubiHSM 2 or YubiHSM 2 FIPS fits easily into a USB slot and lies almost flush to accommodate physical security enclosures.

- "Nano" form-factor enables flexible deployment and use across devices and locations
- Fully concealed USB-A port deployment
- Network shareable for use by applications on other servers

Protection for cryptographic keys with the world's smallest hardware security module (HSM)

Thank you for downloading this Yubico white paper. Carahsoft is the master government aggregator and distributor for Yubico's Cybersecurity solutions available via ILTPP, MHEC, NJSBA, and other contract vehicles.

To learn how to take the next step toward acquiring Yubico's solutions, please check out the following resources and information:

For additional resources:
carah.io/YubicoResources

For upcoming events:
carah.io/YubicoEvents

For additional Yubico solutions:
carah.io/YubicoSolutions

For additional CyberSecurity solutions:
carah.io/CyberSecuritySolutions

To set up a meeting:
Yubico@carahsoft.com
844-214-4790

To purchase, check out the contract vehicles available for procurement:
carah.io/YubicoContracts

yubico

Protection for cryptographic keys with the world's smallest hardware security module (HSM)

The YubiHSM 2 is available as a FIPS 140-2 validated, Level 3 solution, or as a non-FIPS solution, both with the same capabilities. Both solutions ensure uncompromised cryptograhic hardware security for applications, servers and computing devices at a fraction of the cost and size of traditional HSMs.

Cryptographic Keys Stored in Software are Vulnerable to Threats

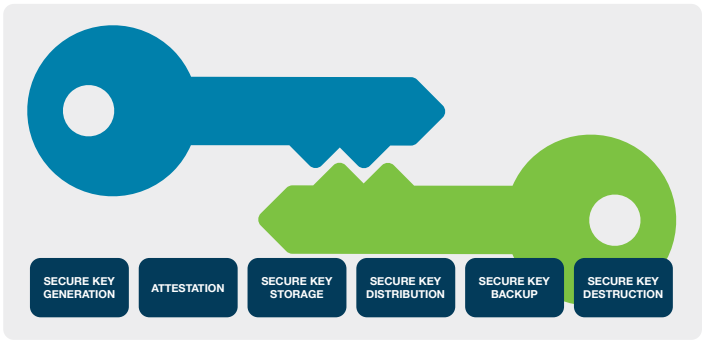
The cost of global cybercrime expected to be $6 trillion in 2021, an increase from $3 trillion 2015.[1] Software storage of cryptographic keys for servers is increasingly vulnerable as attacks become more sophisticated. For example, if a private key is compromised from a Certificate Authority (CA), an attacker can pretend to be your website.

The YubiHSM 2 and YubiHSM 2 FIPS Change the Game for Effective Key Security

Ensure secure hardware cryptographic key storage and operations for applications, servers and computing devices while eliminating the cost and complexity of traditional Hardware Security Modules (HSM)s. Yubico's HSM solutions are tamper resistant and offer low cost, high security ROI in a portable 'nano' form-factor that allow flexible use across diverse devices and locations. With the YubiHSM 2 and YubiHSM 2 FIPS, organizations can prevent cryptographic keys from being copied by attackers, malware and malicious insiders. Enterprises can rapidly integrate with either HSM option using the open source SDK 2.0.

Secure Hardware Protection for Cryptographic Keys

Cryptographic keys stored in software can be copied, and are vulnerable to accidental distribution and remote theft. Without strict procedures, it is easy for admins or malicious insiders to backup keys to USB flash drives, FTP them, or share to others via a cloud storage service. Additionally, sophisticated attackers can gain admin access or deploy trojan malware that installs on servers, searches for cryptographic keys, and then copies them for sale on dark web sites like Alphabay.



Securing the Cryptographic Key Lifecycle

The hardware-based HSM solutions enable secure key storage and operations by preventing accidental copying and distribution of keys, and by preventing remote theft of keys stored.

- Secure key storage and operations on tamper-resistant hardware, with audit logging.
- Extensive cryptographic capabilities including hashing, key wrapping, asymmetric signing, decryption, attestation and more.

Innovative Design for Flexible Use

Traditional rack mounted and card based HSMs are not practical for many organizations because of issues accommodating the HSM's size and deployment complexity. Additionally, rack space at shared data centers often includes physical server enclosures with metal mesh doors to secure access restricting available space.

With Yubico's HSM solutions organizations can easily secure servers, applications, databases, assembly lines, IoT devices, cryptocurrency exchanges and more with a portable 'nano' form factor that allows fast and flexible deployment across diverse environments.

The YubiHSM 2 or YubiHSM 2 FIPS fits easily into a USB slot and lies almost flush to accommodate physical security enclosures.

- 'Nano' form-factor enables flexible deployment and use across devices and locations
- Fully concealed USB-A port deployment
- Network shareable for use by applications on other servers

[1] Cybersecurity Ventures

Low-cost, High Security ROI

Cryptographic keys stored in software are susceptible to hackers and malware attacks. Alternately, traditional HSMs can be costly to deploy.

With Yubico's HSM solutions organizations get enterprise-grade high cryptographic security and operations without the traditional HSM price tag.

- Significant Capex reduction: up to 90% cheaper than traditional HSMs
- Low-power usage device reduces business energy consumption

Rapid Integration, Easy Management

With the YubiHSM 2 SDK, developers can rapidly integrate support for either the FIPS or non-FIPS version of the HSM into business products and applications with capabilities like generating and importing keys, signing and verification, and data encryption and decryption. Developers can also make these features accessible through industry standard PKCS#11.

- Custom application support using open source libraries. Interfaces via YubiHSM KSP, PKCS#11, and native libraries
- Remote management reduces management complexity and costs

Address Existing and Emerging Use Cases

Secure Cryptocurrency Exchanges: The cryptocurrency market is growing rapidly, with a high volume of assets needing protection against emerging security risks. Several exchanges have been breached, all of which may have been prevented with a best practices security approach involving a hardware security module. With the YubiHSM 2 SDK, developers building solutions for cryptocurrency exchanges can rapidly integrate the HSM to protect cryptographic keys and keep sensitive financial information safe.

Secure Internet of Things (IoT) Environments: The Internet-of-Things (IoT) is a rapidly emerging area where systems often operate in hostile environments.[2] Cryptographic keys are used in numerous IoT applications, with insufficient security in place. This is partly because protecting cryptographic keys and enrolling certificates on IoT gateways or proxies has been complicated, and traditional HSMs are too large and unwieldy for certain IoT environments, such as connected cars. With the open source SDK, developers building IoT applications can rapidly integrate with the ultra portable YubiHSM 2 or YubiHSM 2 FIPS to protect cryptographic keys and keep critical IoT environments from falling victim to hostile takeovers.

Secure Cloud Services: Strong security for cloud environments is critical as organizations need to ensure that their data will be kept safe in the cloud. The HSM can be deployed in a data center and run as a component of a cloud infrastructure. Organizations can gain peace of mind knowing that the cloud hosting service of their choice is running the YubiHSM 2 or YubiHSM 2 FIPS as part of their offering.

Secure Microsoft Active Directory Certificate Services: The HSM solution can provide hardware backed keys for an organization's Microsoft-based PKI implementation. Deploying the HSM to the Microsoft Active Directory Certificate services not only protects the Certificate Authority private keys but also protects all signing and verification services using the private key.[3]

Summary

The YubiHSM 2 and YubiHSM 2 FIPS enable organizations of all sizes to enhance cryptographic key security throughout the entire lifecycle, reduce risk and ensure adherence with compliance regulations. With the YubiHSM SDK 2.0 available as open source, organizations can easily and rapidly integrate support for the secure HSM into a wide range of platforms and systems for existing and emerging use cases where strong security is more critical than ever before.

[2] https://www.smartcard-hsm.com/2017/02/14/IoT_Devices_with_SmartCard-HSM.html

[3] Note: All aspects of the YubiHSM 2 SDK 2.0 are available as open source except the Key Storage Provider (KSP) for use with Microsoft Active Directory Certificate Services

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088