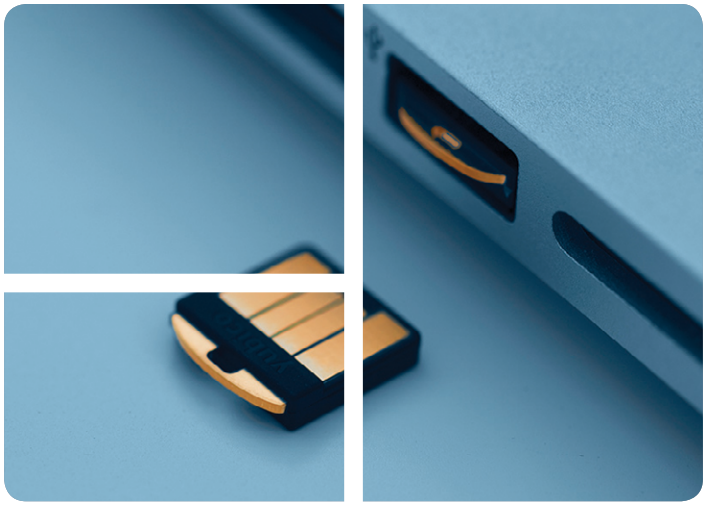
yubico

YubiHSM 2 - Secures Cryptographic Keys

The YubiHSM 2 is a dedicated hardware security module (HSM) that offers superior protection for private keys against theft and misuse.



Cryptographic Keys Stored in Software are Vulnerable to Threats

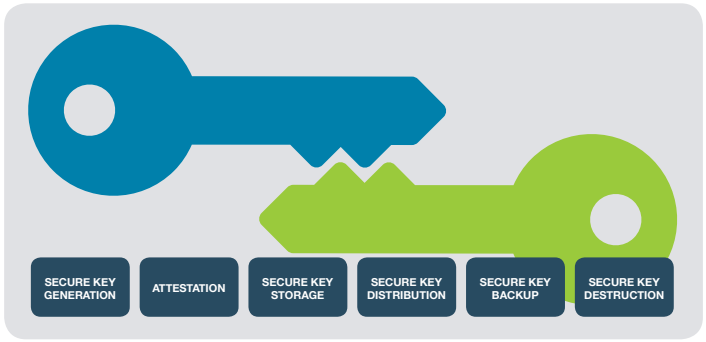
Security breaches are a growing industry wide problem that in 2018 cost companies an average of $3.8 million per breach[1]. Software storage of cryptographic keys for servers is increasingly vulnerable as attacks become more sophisticated. Stolen cryptographic keys from a server may lead to a catastrophic security breach. For example, if a private key is compromised from a Certificate Authority (CA), an attacker can pretend to be your website. With potential damages far exceeding an average breach, necessitating shutdown of all servers, end user systems, and user access for days or weeks complicating recovery, strong security for cryptographic private keys is of greater importance than ever before.

The YubiHSM 2 Changes the Game for Effective Key Security

Traditionally, organizations have used Hardware Security Modules (HSMs) that were costly and complex to set up. However, with the YubiHSM 2, organizations of all sizes can enable effective security for cryptographic keys, across the entire lifecycle, in a portable and affordable hardware form factor. With the YubiHSM 2, organizations can prevent cryptographic keys from being copied by attackers, malware and malicious insiders.

YubiHSM 2 Delivers Enhanced Security and Practical Deployment

The YubiHSM 2 offers a cost effective HSM solution that enables simplified deployment and enables secure key storage and operations. Enterprises can rapidly integrate with the YubiHSM 2 using the open source SDK 2.0 which delivers the following security benefits



Securing the Cryptographic Key Lifecycle

Enhanced Protection for Cryptographic Keys

- **Prevent Poor Cryptographic Key Handling:** Cryptographic keys stored in software can be copied and are vulnerable to accidental distribution. Without strict procedures, it is easy for admins or malicious insiders to copy keys to USB flash drives for backup purposes, ftp them, or share to others via a cloud storage service. Once that happens, the cryptographic keys may be forgotten on a USB drive or end up stored indefinitely in an external service or system. The keys could even be left on the drive of an old server queued for recycle. The hardware-based YubiHSM 2 offers superior security by preventing accidental copying and distribution of cryptographic keys.
- **Prevent Remote Theft of Keys:** Cryptographic keys stored in software are also vulnerable to remote theft. Sophisticated attackers can gain admin access or deploy trojan malware that installs on servers, searches for cryptographic keys, then copies them for sale and distribution on dark web sites like Alphabay. Storing cryptographic keys in the YubiHSM 2 offers superior hardware-based security and eliminates malware and remote attackers from being able to extract the private keys.

[1] 2018 Cost of Data Breach Study, Ponemon Institute Research Report

Rapid Integration with Hardware-Based Strong Key Security

- **Gain a comprehensive cryptographic toolbox:** With the YubiHSM 2 SDK, developers can rapidly integrate support for the YubiHSM 2 into the products and services being built. The YubiHSM 2 SDK brings the capabilities of the YubiHSM 2 to life such as generating and importing keys, signing and verification, and encrypting and decrypting data. for open source and commercial applications spanning many different products and services. Most common use cases involve on-chip hardware based processing for signature generation and verification.
- **Support for PKCS#11:** Using the YubiHSM 2 SDK, developers can easily make the YubiHSM 2 features accessible through industry standard PKCS#11. As most commercial certificate authority software uses PKCS #11 to access the CA signing key or to enroll user certificates, support for PKCS#11 enables organizations to address the use cases that have this requirement.

Practical and Simplified Deployment for Organizations of All Sizes

- **Enterprise-grade protection in a portable and affordable form factor:** Traditional rack mounted and card based HSMs are not practical for many organizations because of issues accommodating the HSM's deployment complexity, or its cost. Additionally, rack space at shared data centers often includes physical server enclosures with metal mesh doors to secure access. As the world's smallest HSM the YubiHSM 2 fits easily into a front USB slot on servers and lies almost flush to accommodate these physical security enclosures, and can be deployed in hours, not days.

Address Existing and Emerging Use Cases

Secure Cryptocurrency Exchanges: The cryptocurrency market is rapidly growing with market valuation expected to hit $1 trillion in 2018. With this explosive growth also comes a high volume of assets that need protection to mitigate against emerging security risks. Several exchanges have been breached, with the number growing steadily, 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 YubiHSM 2 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. That makes securing cryptographic keys even more important as organizations need to protect sensitive information. 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 to protect cryptographic keys nd 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 YubiHSM 2 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 as part of their offering.

Secure Microsoft Active Directory Certificate Services: The YubiHSM 2 can provide hardware backed keys for an organization's Microsoft-based PKI implementation. Deploying YubiHSM 2 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.

Summary

The YubiHSM 2 enables 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 YubiHSM 2 into a wide range of platforms and systems for existing and emerging use cases where strong security is more critical than ever before.

Yubico AB
Olof Palmes gata 11
6th floor
SE-111 37 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088

[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