YubiHSM 2 Product Overview

Yubico

Jul 08, 2022

CONTENTS

CHAPTER

ONE

INTRODUCTION

1.1 What is YubiHSM 2?

The YubiHSM 2 is a Hardware Security Module (HSM) that is cost-effective for all organizations. It provides advanced cryptography including hashing, asymmetric, and symmetric key cryptography to protect the cryptographic keys that secure critical applications, identities, and sensitive data in an enterprise for certificate authorities, databases, code signing and more.

Important: The FIPS certification of the YubiHSM 2 [FIPS 140-2 Level 3] is recorded on the website of the National Institute of Standards and Technology at https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3916.

1.2 System Requirements

The YubiHSM 2 SDK is built and provided for the following operating systems.

Operating System	Version	Architecture
CentOS	7	amd64
CentOS	8	amd64
Debian	9 Stretch (stable)	amd64
Debian	10 Buster	amd64
Debian	11 Bullseye	amd64
Fedora	33	amd64
Fedora	34	amd64
Ubuntu	14.04 Trusty Tahr	amd64
Ubuntu	16.04 Xenial Xerus	amd64
Ubuntu	18.04 Bionic Beaver	amd64
Ubuntu	20.04 Focal Fossa	amd64
Ubuntu	21.04 Hirsute Hippo	amd64
Ubuntu	21.10 Impish Indri	amd64
Windows	Server 2019	x64, x86
macOS	10.15 Catalina, 11 Big Sur	amd64, arm64, universal

1.3 License

The YubiHSM 2 SDK is intended for use in development and production environments in conjunction with YubiHSM 2, pursuant to Yubico Toolset Software License Agreement. By downloading and installing the SDK you agree to the terms of this license.

The released SDK source code is licensed under the Apache 2.0 license.

Third party software included in the YubiHSM 2 SDK, and their respective licenses, are listed in the licenses directory inside the SDK package.

1.4 The YubiHSM 2 Device

The YubiHSM 2 is a USB-based, multi-purpose cryptographic device for servers. Its diminutive physical size is ideal for installation directly into internal or external server ports.

1.5 What's in the SDK

The SDK contains tools to interface with YubiHSM 2. For more information about each of the main components, please see the component reference section.

Resource	Description
bin/libcrpto-1_1-x64.dll	Pre-built OpenSSL (Windows only)
bin/yubihsm-setup	Deployment tool for YubiHSM 2
bin/yubihsm-wrap	A tool to create wrapped importable objects offline
bin/yubihsm-connector	The connector, a tool for providing a common interface to the device
bin/yubihsm-shell	The shell, a REPL-style tool for interacting with YubiHSM 2 (and the connector) See **Note (1)**
include/pkcs11/pkcs11.h	Common and standard PKCS#11 functions and constants definitions
include/pkcs11/pkcs11y.h	Yubico-specific PKCS#11 functions and constants definitions
include/yubihsm.h	Library functions and constants definitions
lib/libyubihsm.{dylib,so} or in/libyubihsm.dll	Library binary to interact with YubiHSM 2
lib/yubihsm_pkcs11.{dylib,so} or bin/yubihsm_pkcs11.dll	PKCS#11 module to interact with ubiHSM 2
python-noarch/*	Python implementation of the library
yubihsm-cngprovider-windows-amd64.msi	Installer for CNG/KSP for Windows ADCS (Windows only)
yubihsm-connector-windows-amd64.msi	Installer for the connector (Windows only)

Note (1) Read-Evaluation-Print-Loop, REPL

1.6 YubiHSM 2 FIPS

The YubiHSM 2 is FIPS 140-2 certified and listed on the NIST site under Certificate 3916. YubiHSM 2 FIPS devices include the text "FIPS" laser-etched onto the surface of the device, and support the FIPS Approved mode flag.

Placing a YubiHSM 2 into FIPS mode will require that all loaded objects have been deleted, which can be performed via a "Reset Device" command.

1.6.1 Putting into FIPS Mode

To configure the YubiHSM 2 into the FIPS Approved mode of operation:

Step 1
Use the "Set Option" service as follows: 4f000405000101 or `put option 0 fips-mode 01`.

Step 2
Import new Authentication Keys to replace the default values.

1.6.2 Validating the Mode

To check the mode of operation:

Use the "Get Option" service as follows: `get option 0 fips-mode`

- `01` return code indicates the Approved mode
- `00` return code indicates the non-Approved mode

1.6.3 Taking it out of FIPS Mode

To configure the YubiHSM 2 into the non-Approved mode of operation:

Step 1
Delete all objects on the YubiHSM 2.

Step 2
Use the "Set Option" service as follows: 4f000405000100 or `put option 0 fips-mode 00`.

1.7 Getting Help

Documentation aiding in deploying and using the YubiHSM 2 is continuously updated on https://docs.yubico.com/ (this site). Additional support resources are available in the Yubico Knowledge Base.

Important: If you think you may have discovered a flaw in the product, Yubico welcomes your feedback. To report an issue that you suspect might be a bug, please submit a support request and provide as much detail as you can.

To submit a support request: https://support.yubico.com/hc/en-us

CHAPTER

TWO

DOCUMENTATION OVERVIEW

The purpose of this documentation is both to provide detailed descriptions of YubiHSM 2 concepts and to function as a reference for commands and APIs provided. Before setting up YubiHSM 2 for the first time, familiarize yourself with the basic concepts and terminology used in the product documentation contained within these pages as well as in the software itself.

Note: The YubiHSM 2 SDK documentation and usage guides are enhanced continuously. Please check back regularly to see what is new.

- Releases provides access to release notes, downloads, resolved and known issues, and limitations.
- Product Overview (this section) gives a high-level description of the YubiHSM 2 offering; product specifications, contents of the SDK, and how to get help.
- Concepts explains the foundational concepts used; understanding of these concepts is necessary in order to use YubiHSM 2.
- Commands provides an inventory of all available commands, with yubihsm-shell usage examples.
- Component Reference is a collection of reference materials for the components included in the SDK:
  - The core libraries
  - The PKCS#11 module
  - The Shell
  - The Key Storage Provider, and more.
- Back Up and Restore. The YubiHSM 2 supports encrypted export and import of objects using a symmetric AES-CCM based scheme.
  - Additional information on backing up and restoring is provided by:
    * Backing up and Restoring Keys in YubiHSM 2 Administration and Usage Guides;
    * Back Up and Restore Key Material in YubiHSM 2 with Key Storage Provider for Windows Server;
    * Backing Up Key Material in Deploying YubiHSM 2 with ADCS.
- Usage Guides supply a number of examples for using the YubiHSM 2:
  - YubiHSM 2 Administration and Usage Tasks,
  - YubiHSM 2 for Active Directory Certificate Services Guide,
  - Introduction to YubiHSM 2 with Key Storage Provider for Windows Server,
  - YubiHSM 2 for MS Host Guardian Service Guide, and

- YubiHSM 2 for MS SQL Server Guide

CHAPTER

THREE

SPECIFICATIONS

3.1 Cryptographic Interfaces

- PKCS#11 API version 2.40
- Yubico Key Storage Provider (KSP) to access Microsoft CNG. The KSP is provided as 64-bit and 32-bit DLLs
- Full access to device capabilities through Yubico's YubiHSM Core Libraries (C, Python)

3.2 RSA

- 2048, 3072, and 4096 bit keys (with e=65537)
- Signing using PKCS#1v1.5 and PSS
- Decryption using PKCS#1v1.5 and OAEP

3.3 Elliptic Curve Cryptography (ECC)

- **Curves**: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, Ed25519
- **Signing**: ECDSA (all except Ed25519), EdDSA (Ed25519 only)
- **Derivation**: ECDH (all except Ed25519)

3.4 Hashing Functions

SHA-1, SHA-256, SHA-384, SHA-512

3.5 Key Wrap

Import and export using NIST-approved AES-CCM Wrap with 128, 196, and 256 bit keys

3.6 Random Numbers

On-chip True Random Number Generator (TRNG) used to seed NIST SP 800-90A Rev.1 AES-256 CTR_DRBG

3.7 Attestation

Asymmetric key pairs generated on-device may be attested using a device-specific Yubico attestation key and certificate, or using your own keys and certificates imported into the HSM.

3.8 Performance

Performance varies depending on usage. The accompanying Software Development Kit includes performance tools that can be used for additional measurements. Example metrics from an otherwise unoccupied YubiHSM 2:

- RSA-2048-PKCS1-SHA256: ~139ms
- RSA-3072-PKCS1-SHA384: ~504ms
- RSA-4096-PKCS1-SHA512: ~852ms
- ECDSA-P224-SHA1: ~64ms
- ECDSA-P256-SHA256: ~73ms
- ECDSA-P384-SHA384: ~120ms
- ECDSA-P521-SHA512: ~210ms
- EdDSA-25519-32Bytes: ~105ms
- EdDSA-25519-64Bytes: ~121ms
- EdDSA-25519-128Bytes: ~137ms
- EdDSA-25519-256Bytes: ~168ms
- EdDSA-25519-512Bytes: ~229ms
- EdDSA-25519-1024Bytes: ~353ms
- AES-(128|192|256)-CCM-Wrap: ~10ms
- HMAC-SHA-(1|256): ~4ms
- HMAC-SHA-(384|512): ~243ms

3.9 Storage Capacity

- All data stored as objects. 256 object slots, 126KB max total
- Stores up to 127 rsa2048 or 93 rsa3072 or 68 rsa4096 or 255 of any elliptic curve type, assuming only one authentication key is present
- Object Types: Authentication keys (used to establish sessions); Asymmetric private keys; Opaque binary data objects (e.g. x509 certificates); Wrap keys; HMAC keys

3.10 Management

- Mutual authentication and secure channel between applications and the YubiHSM 2
- M of N unwrap key restore via YubiHSM Setup Tool

3.11 Physical Characteristics

- **Form factor**: *nano* designed for confined spaces such as internal USB ports in servers
- **Dimensions:** 12mm x 13mm x 3.1mm
- **Weight:** 1g

3.12 Temperatures

- **Operational range:** 0°C - 40°C (32°F - 104°F)
- **Storage range:** -20°C - 85°C (-4°F - 185°F)

3.13 Host Interface

Universal Serial Bus (USB) 1.x Full Speed (12Mbit/s) Peripheral with bulk interface

CHAPTER

FOUR

COPYRIGHT

© 2022 Yubico AB. All rights reserved.

Trademarks

Yubico and YubiKey are registered trademarks of Yubico AB. All other trademarks are the property of their respective owners.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

Contact Information

Yubico Inc.
530 Lytton Street
Suite 301
Palo Alto, CA 94301
USA

Click the links to:

- Submit a support request
- Send a Contact Me request
- See additional contact options for getting touch with us

Document Updated

2022-07-08 20:08:31 UTC