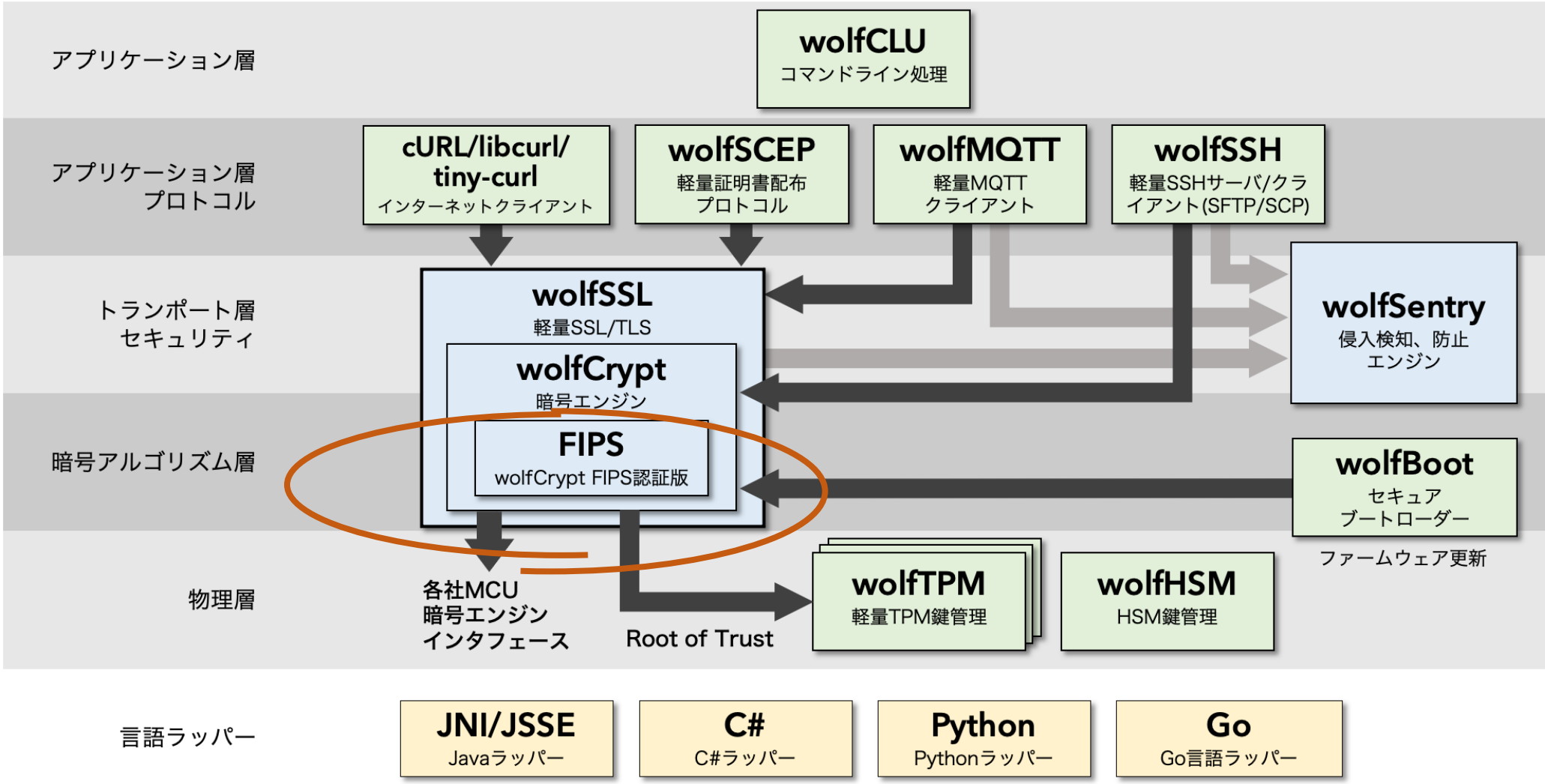
ウチの製品をFIPS認証取得済にするためのすべて

wolfSSL Japan合同会社
2024年11月7日
古城　隆

アジェンダ

1. はじめに
2. FIPS認証とは
3. wolfSSLの認証取得サポート
    - wolfSSLユーザ
    - OpenSSLユーザ
4. よくある質問

製品体系


アプリケーション層
wolfCLU
コマンドライン処理
アプリケーション層
プロトコル
cURL/libcurl/
tiny-curl
インターネットクライアント
wolfSCEP
軽量証明書配布
プロトコル
wolfMQTT
軽量MQTT
クライアント
wolfSSH
軽量SSHサーバ/クライアント(SFTP/SCP)
トランポート層
セキュリティ
wolfSSL
軽量SSL/TLS
wolfCrypt
暗号エンジン
FIPS
wolfCrypt FIPS認証版
wolfSentry
侵入検知、防止
エンジン
暗号アルゴリズム層
wolfBoot
セキュア
ブートローダー
ファームウェア更新
物理層
各社MCU
暗号エンジン
インタフェース
Root of Trust
wolfTPM
軽量TPM鍵管理
wolfHSM
HSM鍵管理
言語ラッパー
JNI/JSSE
Javaラッパー
C#
C#ラッパー
Python
Pythonラッパー
Go
Go言語ラッパー

FIPS認証とは

- 米国連邦政府の情報機器調達基準(非軍事利用)
  米国NISTとカナダCSECの共同運営

- FIPS140
  セキュリティー、暗号モジュールに関する認証基準
  Federal Information Processing Standard Publication
  National Institute of Standards and Technology (NIST)
  - 140-2: 2001年5月初版
  - 140-3: 2019年9月発効、2024年移行

- セキュリティレベル
  - レベル1: **基本レベル**の安全性
    ソフトウェア、ファームウェア
  - レベル2: ハードウェア耐タンパー性
  - レベル3: 物理的攻撃の検出、対抗処置
  - レベル4: 環境耐性

認証プログラム

- CAVP: Cryptographic Algorithm Validation Program
  - 暗号アルゴリズムごとのKAT(Know Answer Test)

    認定テストラボが提供するテストベクターによるテストと結果の検証
  - NIST認定のCST(Cryptographic and Security Testing) Labのみが実施

- CMVP: Cryptographic Module Validation Program
  - CAVPテスト
  - テストプログラムの実装

    - POST（Pre-operational Self-Test)

      運用前セルフテスト

      バイナリコードのMACチェック、最小限のアルゴリズムKAT

    - CAST (140-3: Conditional Algorithm Self-Testing)

      アルゴリズム使用前KAT

wolfSSLのFIPS: 対象アルゴリズム

- ハッシュ：　SHA-2/3
- 認証コード：CMAC/HMAC-SHA2/SHA3
- 共通鍵：　AES-ECB/CBC/CCM/CTR/GCM
- 公開鍵暗号：RSA KeyGen/Enc/Dec
- 公開鍵合意：KAS ECC CDH/ECC SSC/FFC
- 公開鍵署名：RSA KeyGen/Sig/Ver, DSA KeyGen/Sig/Ver
  ECDSA KeyGen/Sig/Ver
- 鍵導出：　TLS v1.3/v1.2 KDF, SSH KDF
- 乱数：　Hash DRBG

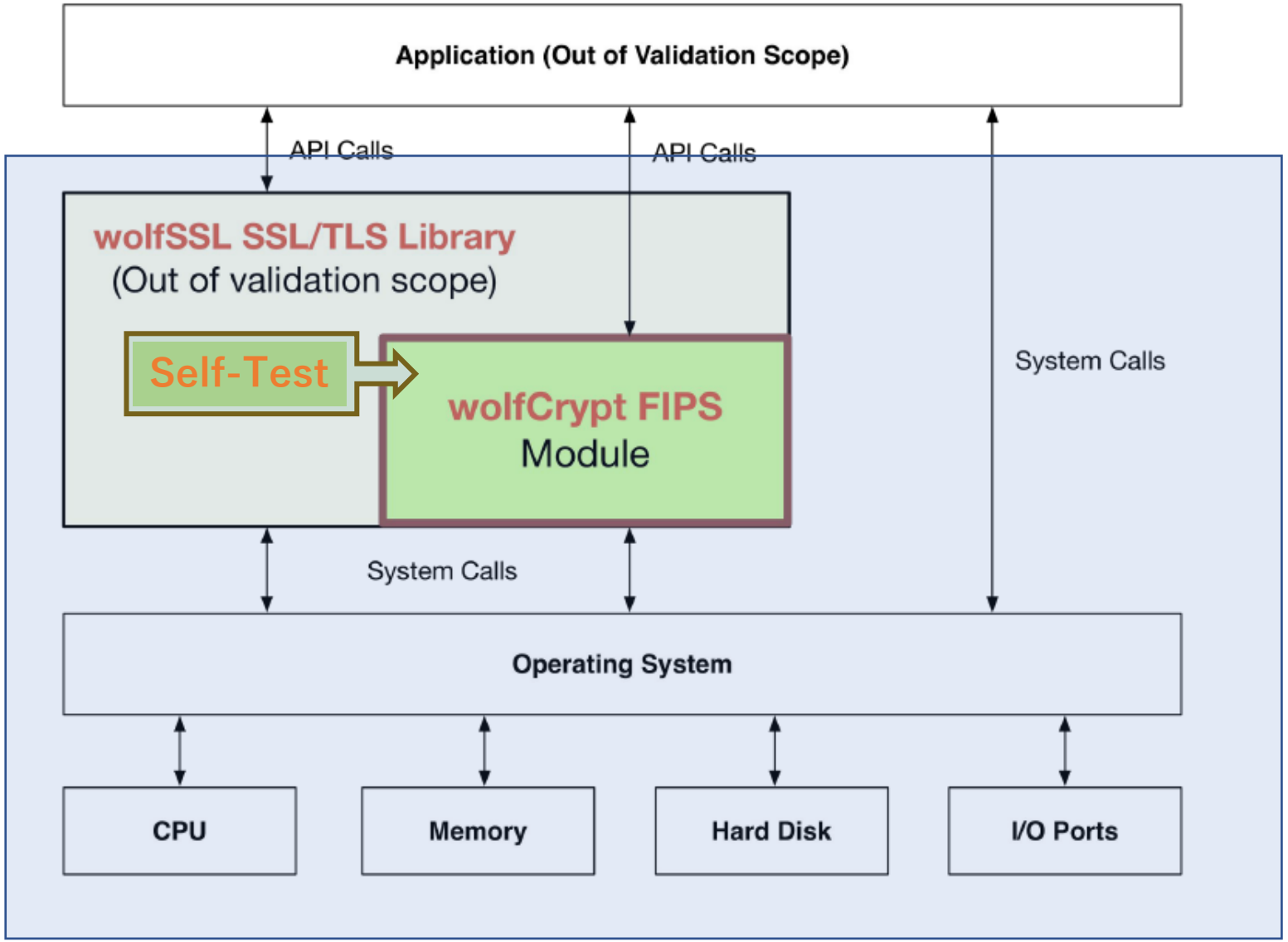
運用前自己テスト(Pre-Operation Self-Test)

- (電源投入時など)全ての処理に先立つ自己テスト(Self test)
- ライブラリのロード時にテストを自動実行
- 実行イメージのMAC値をチェック（改ざん検出）
- HMAC実行に必要なアルゴリズムに対して既知の回答テスト(KAT)を実行
- 失敗した場合、すべてのアルゴリズム機能をロックアウト

CAST (Conditional Algorithm Self-Testing)

- FIPS140-3で導入
- ブート時間の短縮
  - POSTではMAC検証に使用するアルゴリズムのKATのみ
  - 各アルゴリズム使用直前までにKATを実施
  - wolfCrypt　API内で要否を判定。該当CASTを自動実行
- CASTフェイル時の縮退運用が許される

Crypt Boundaryとセルフテスト



実行環境(OE: Operating Environment)

認証の対象となる実行環境の定義

- チップセット

例：Intel® CoreTM i7-7820 @2.9GHz x 4 with AES-NI

- OS

例：Windows 10 Enterprise

- 暗号モジュール

例：wolfCrypt v5.7.2

- **お客様のOEごと**に検証必要

CMVP認証：フルサブミッション

最初の認証取得。一連のアルゴリズムセットを検証

Certificate #4718

OEUP: OEを追加

複数のOE上で一連のアルゴリズムセットを検証

Certificate #4718

CMSIS-RTOS2 v2.1.3 running on Alto™ with Silicon Labs EFM32G (Gecko)
CodeOS v1.4 running on Series CR2700 Code Reader(s) with CodeCorp CT8200 (ARM FA626TE)
Fusion Embedded ROTS 5.0 running on Classone ® IP Radio Gateway with Analog Devices ADSP-BF516 (BlackFin)
HP Imaging & Printing Linux 4.9 running on HP PN 3PZ95-60002 with ARM Cortex-A72 with PAA
HP Imaging & Printing Linux 4.9 running on HP PN 3PZ95-60002 with ARM Cortex-A72 without PAA
Linux 4.12 Yocto Standard running on Metasys® SNC Series Network Control Engine with Freescale i.MX6 DualLite ARMv7 Cortex-A9 x2 with PAA
Linux 4.12 Yocto Standard running on Metasys® SNC Series Network Control Engine with Freescale i.MX6 DualLite ARMv7 Cortex-A9 x2 without PAA
Linux 4.14 running on SEL-2742S with an ARMv8 Cortex A53 with PAA
Linux 4.14 running on SEL-2742S with an ARMv8 Cortex A53 without PAA
Linux 4.19 running on Cloudworx Video ENC-DEC with ARMv8 Cortex A53 with PAA
Linux 4.19 running on Cloudworx Video ENC-DEC with ARMv8 Cortex A53 without PAA
Linux 4.4 (Ubuntu 16.04 LTS) running on Intel Ultrabook 2 in 1 with an Intel® Core™ i5-5300U CPU @2.30GHz x 4 with PAA
Linux 4.4 (Ubuntu 16.04 LTS) running on Intel Ultrabook 2 in 1 with an Intel® Core™ i5-5300U CPU @2.30GHz x 4 without PAA
Linux socfpga Cyclone V running on SEL 2700 Series 24-Port Ethernet Switch with an ARMv7 rev0, Cortex A-9
Nucleus 3.0 version 2013.08.1 running on XL200 Radio with CodeCorp CT8200 (ARM FA626TE)
OpenRTOS v10.1.1 running on STMicroelectronics STM32L4R9I-DISCO (Discovery Kit) with a STMicroelectronics STM32L4Rx
Red Hat Enterprise Linux Workstation running on DELL Precision 5820 with an Intel® Xeon™ W-2155 @ 3.3GHz x 20 with PAA
Red Hat Enterprise Linux Workstation running on DELL Precision 5820 with an Intel® Xeon™ W-2155 @ 3.3GHz x 20 without PAA
Windows 10 Enterprise running on Radar FCL Package Utility with Intel® Core™ i7-7820 @2.9GHz x 4 with PAA
Windows 10 Enterprise running on Radar FCL Package Utility with Intel® Core™ i7-7820 @2.9GHz x 4 without PAA

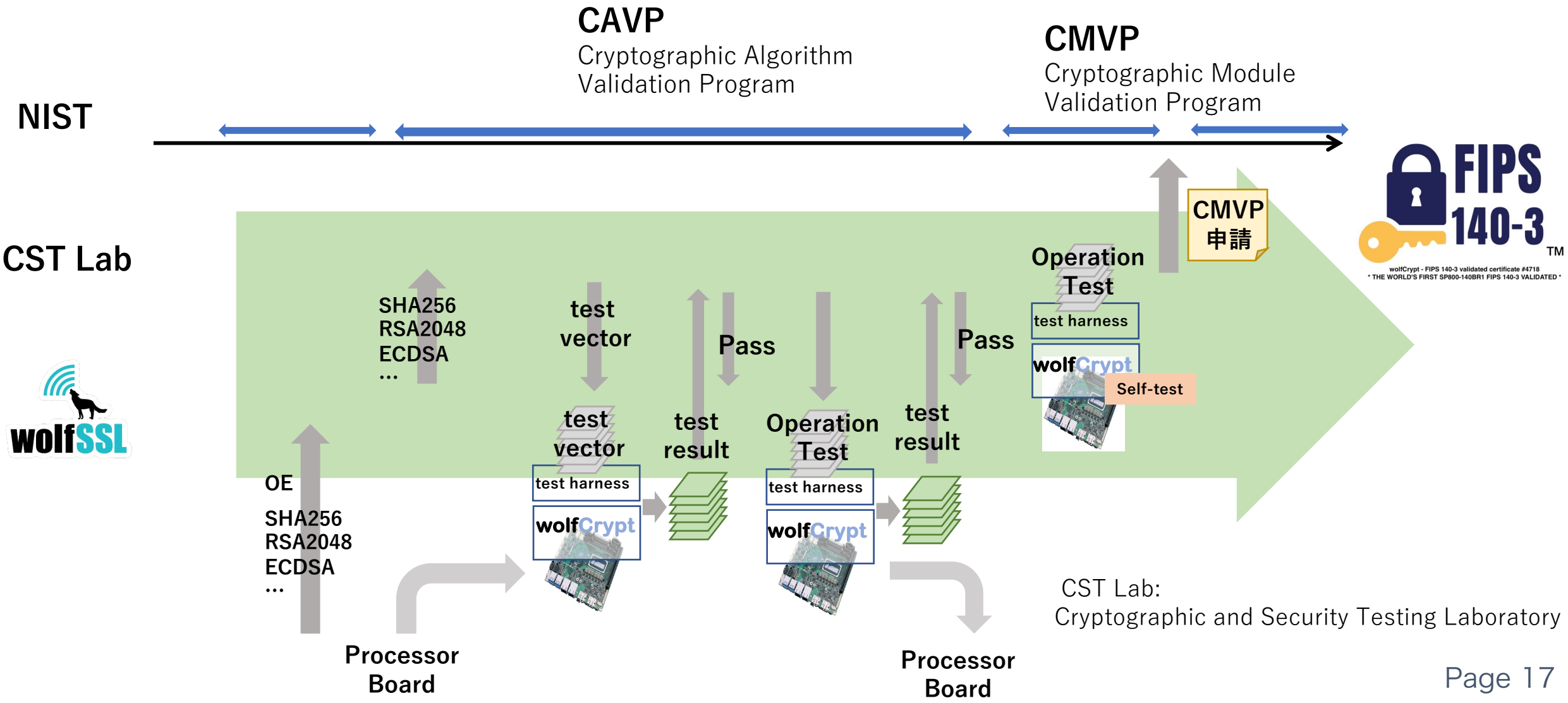
OEUP: OEを追加

認証済のアルゴリズムセットにOEを追加

Certificate #4718

CMSIS-RTOS2 v2.1.3 running on Alto™ with Silicon Labs EFM32G (Gecko)
CodeOS v1.4 running on Series CR2700 Code Reader(s) with CodeCorp CT8200 (ARM FA626TE)
Fusion Embedded ROTS 5.0 running on Classone ® IP Radio Gateway with Analog Devices ADSP-BF516 (BlackFin)
HP Imaging & Printing Linux 4.9 running on HP PN 3PZ95-60002 with ARM Cortex-A72 with PAA
HP Imaging & Printing Linux 4.9 running on HP PN 3PZ95-60002 with ARM Cortex-A72 without PAA
Linux 4.12 Yocto Standard running on Metasys® SNC Series Network Control Engine with Freescale i.MX6 DualLite ARMv7 Cortex-A9 x2 with PAA
Linux 4.12 Yocto Standard running on Metasys® SNC Series Network Control Engine with Freescale i.MX6 DualLite ARMv7 Cortex-A9 x2 without PAA
Linux 4.14 running on SEL-2742S with an ARMv8 Cortex A53 with PAA
Linux 4.14 running on SEL-2742S with an ARMv8 Cortex A53 without PAA
Linux 4.19 running on Cloudworx Video ENC-DEC with ARMv8 Cortex A53 with PAA
Linux 4.19 running on Cloudworx Video ENC-DEC with ARMv8 Cortex A53 without PAA
Linux 4.4 (Ubuntu 16.04 LTS) running on Intel Ultrabook 2 in 1 with an Intel® Core™ i5-5300U CPU @2.30GHz x 4 with PAA
Linux 4.4 (Ubuntu 16.04 LTS) running on Intel Ultrabook 2 in 1 with an Intel® Core™ i5-5300U CPU @2.30GHz x 4 without PAA
Linux socfpga Cyclone V running on SEL 2700 Series 24-Port Ethernet Switch with an ARMv7 rev0, Cortex A-9
Nucleus 3.0 version 2013.08.1 running on XL200 Radio with CodeCorp CT8200 (ARM FA626TE)
OpenRTOS v10.1.1 running on STMicroelectronics STM32L4R9I-DISCO (Discovery Kit) with a STMicroelectronics STM32L4Rx
Red Hat Enterprise Linux Workstation running on DELL Precision 5820 with an Intel® Xeon™ W-2155 @ 3.3GHz x 20 with PAA
Red Hat Enterprise Linux Workstation running on DELL Precision 5820 with an Intel® Xeon™ W-2155 @ 3.3GHz x 20 without PAA
Windows 10 Enterprise running on Radar FCL Package Utility with Intel® Core™ i7-7820 @2.9GHz x 4 with PAA
Windows 10 Enterprise running on Radar FCL Package Utility with Intel® Core™ i7-7820 @2.9GHz x 4 without PAA
Windows 10 running on Intel Ultrabook 2 in 1 with an Intel® Core™ i5-5300U CPU @2.30GHz x 4 with PAA
Windows 10 running on Intel Ultrabook 2 in 1 with an Intel® Core™ i5-5300U CPU @2.30GHz x 4 without PAA ←新たなOEの追加

CAVP/CMVP認証のプロセス：OEの追加



wolfSSLの
認証サポート

サポート暗号アルゴリズム、スキーム

- ハッシュ：　SHA-2/3
- 認証コード：HMAC-SHA2/SHA3
- 共通鍵：　AES-ECB/CBC/CCM/CTR/GCM/CMAC
- 公開鍵暗号：RSA KeyGen/Enc/Dec
- 公開鍵合意：KAS ECC CDH/ECC SSC/FFC
- 公開鍵署名：RSA KeyGen/Sig/Ver, DSA KeyGen/Sig/Ver
  ECDSA KeyGen/Sig/Ver
- 鍵導出：　TLS v1.3/v1.2 KDF, SSH KDF
- 乱数：　Hash DRBG

wolfSSL: FIPS Ready版

- これまでの課題
  - FIPS認証版を利用したいが取得コストがネック
  - 認証はOE(実行環境)依存だが、認証対象のOEが確定していない
  - 見込み顧客が確定してからでは、製品組込内容の変更困難
- FIPS Ready版
  - FIPS版と同一構成だが、認証は未取得

  従って、FIPS認証取得とは言えないけれど

  - GPLv2ライセンス版あり

    → あらかじめ技術評価可能
  - 商用版は標準版に近い価格

    →あらかじめ製品に組込可能
  - 見込み顧客が確定してから、対象OEにて認証取得

OpenSSLユーザのための取得サポート

取得シナリオ：

- wolfSSLのOpenSSL互換APIを利用した移行
- wolfEngine/Providerによる取得サポート

OpenSSL 互換API

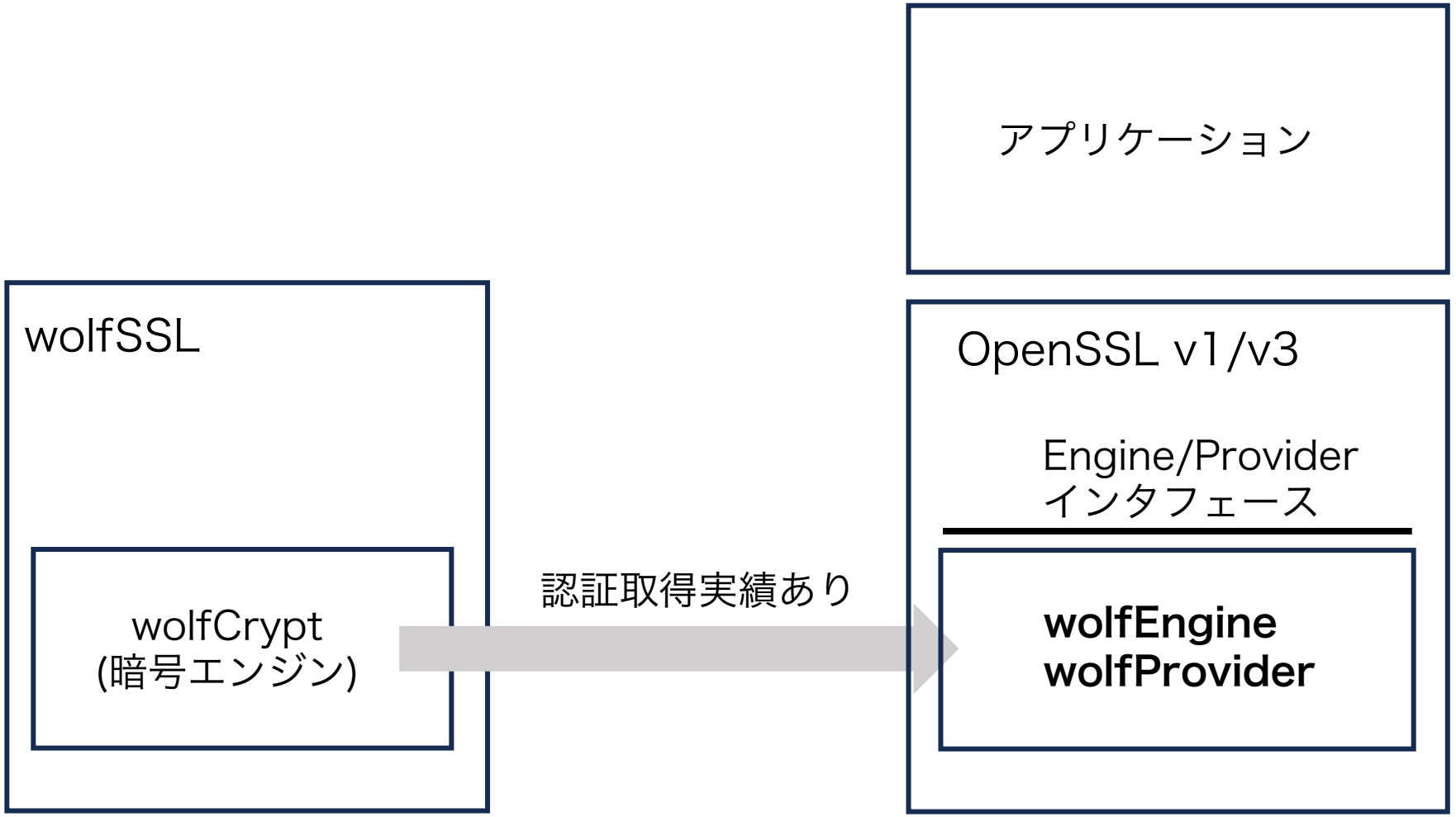
- OpenSSL 上のアプリケーションの速やかな移行
- クリーンルーム独自開発
  OpenSSLその他のIPから完全独立
- APIレベルの互換性
  構造体への直接アクセス等は不可
- 約1,700以上の主要なAPIを実現
- 多数のOSSの移行実績
  MySQL, Nginx, Lighttpd, OpenWRT, stunnel, …

wolfEngine/wolfProvider

目的：
　OpenSSL本体、その上のアプリケーションを
　変更無しにFIPS認証を取得

- OpenSSLのCryptographic Engineを**認証取得実績のある**
  wolfCryptの暗号アルゴリズムに置き換え
  - wolfEngine:　OpenSSL v1
  - wolfProvider: OpenSSL v3
- 既存OpenSSLとの高い互換性を実現
- ただし、お客様によるOpenSSL本体の維持管理が必要

wolfEngine/wolfProvider

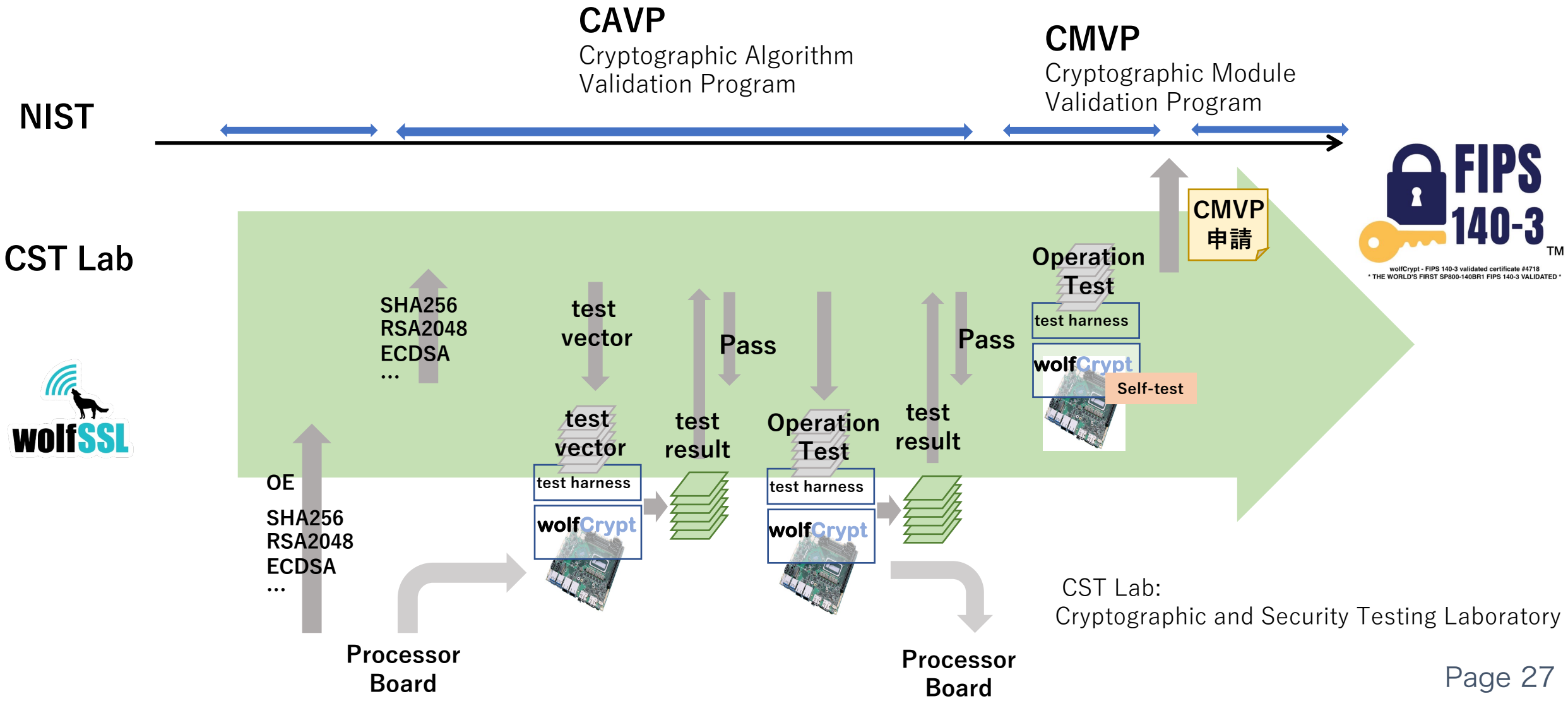


FIPS認証に関するFAQ

FIPS認証に関するFAQ

- wolfSSLのFIPS認証取得サービスを受ける際、
  どんな準備が必要ですか？

CAVP/CMVP認証のプロセス：OEの追加



FIPS認証に関するFAQ

- wolfSSLのFIPS認証取得サービスを受ける際、
  どんな準備が必要ですか？

- 認証対象のアルゴリズムを決定
  wolfSSLでTLS, SSHなどのための標準的なセットを提供
- CAVP/CMVPテストのためのプロセッサボード貸与
- Cプログラミング環境一式の貸与
  OSSツールチェーンの場合はバージョン情報など

FIPS認証に関するFAQ

- ACVPというのも聞きましたが、何ですか？

FIPS認証に関するFAQ

- ACVPというのも聞きましたが、何ですか？

- ACVP（Automated Cryptographic Validation Protocol）は、暗号モジュールの試験や検証を自動化するためのプロトコル。
- NIST, 認証ラボ、サービスベンダー
- お客様があまり意識する必要はない

FIPS認証に関するFAQ

- OEはどういう単位で取得すればいいですか？

FIPS認証に関するFAQ

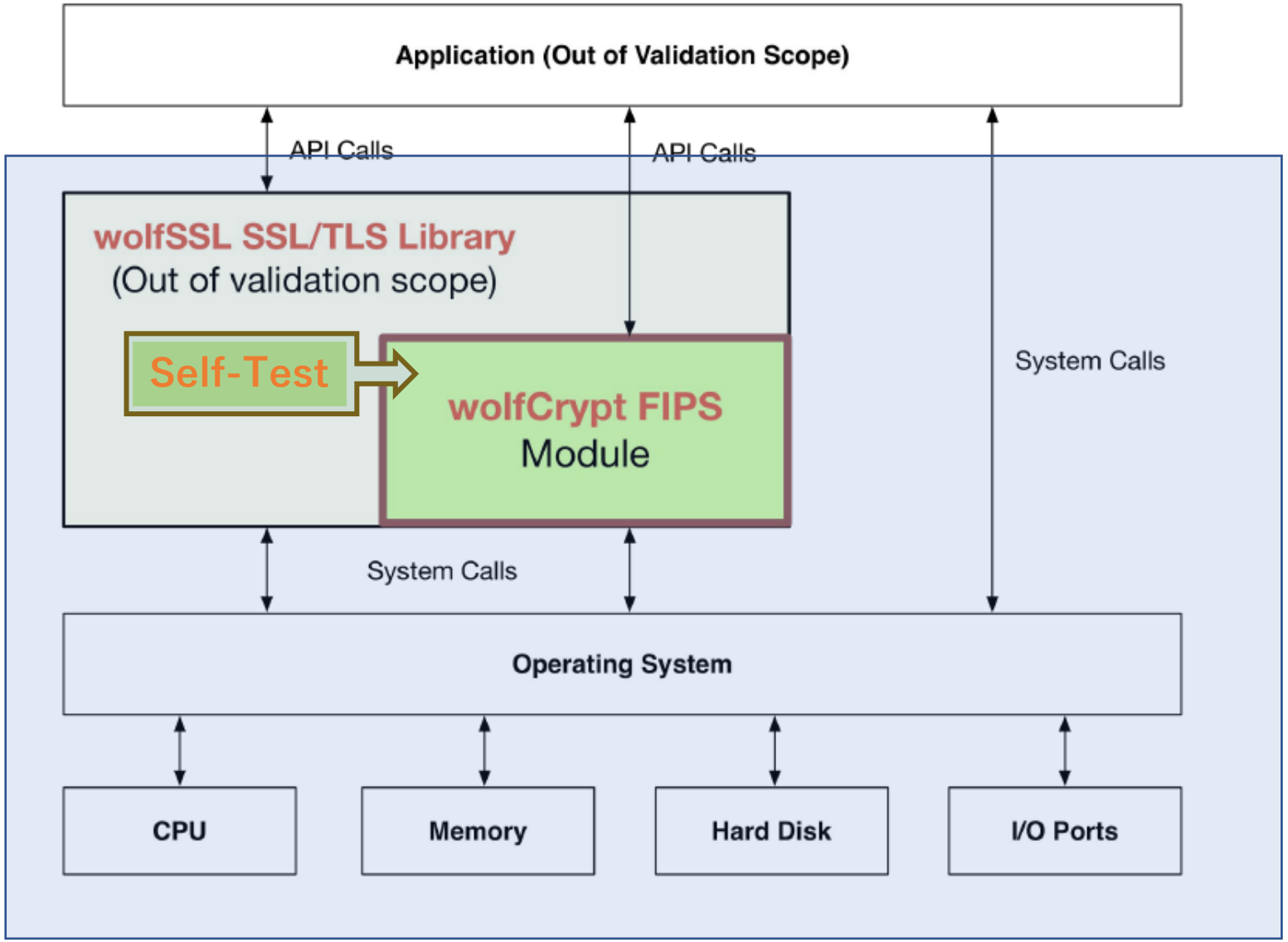
- OEはどういう単位で取得すればいいですか？

- 明文化、公開された規約はなくNISTの運用によるところが大きい。
- NISTサイトにて過去の取得実績も公開されている

FIPS認証に関するFAQ

- 認証取得後にwolfSSL/wolfCryptはまったく変更不可ですか？

Crypt Boundaryとセルフテスト



FIPS認証に関するFAQ

- 認証取得後にwolfSSL/wolfCryptはまったく変更不可ですか？

- 認証対象のソースファイルは変更不可
- ただし、対象はwolfCryptの中の中核となるCrypto Boundary内のソース・ヘッダーファイルのみ。
- それ以外の部分はアップデート可能

FIPS認証に関するFAQ

- 認証の有効期限は?

FIPS認証に関するFAQ

- 認証の有効期限は?

- 有効期限は5年
- 更新のためには、再度認証テストを実施。ただし、フルテストではなく、更新時の状況に応じたテスト

FIPS認証に関するFAQ

- 取得対象アルゴリズムは追加可能ですか?

FIPS認証に関するFAQ

- 取得対象アルゴリズムは追加可能ですか?

可能。ただし、かなりの追加費用と期間。

FIPS認証に関するFAQ

- 自社名での認証取得はできますか？

FIPS認証に関するFAQ

- 自社名での認証取得はできますか？

はい。取得のための費用などご相談ください。


Q&A