wolfHSM:
HSMの実装を容易にするフレームワーク

wolfSSL Japan合同会社
2024年11月7日
古城　隆

もくじ

wolfSSLは…

ネットワークセキュリティ専門ベンダー

wolfSSL

組み込みシステム向け
ソフトウェアライブラリを提供

国内外の政府機関、民間企業

2,000社以上のグローバルカスタマー

wolfSSLの利用分野

産業/ビジネス機器：
- 金融決済端末
- スマートファクトリ
- FA機器、産業用ロボット
- 電力監視
- ビル管理
- 複合機、プリンタ
- アプライアンスボックス

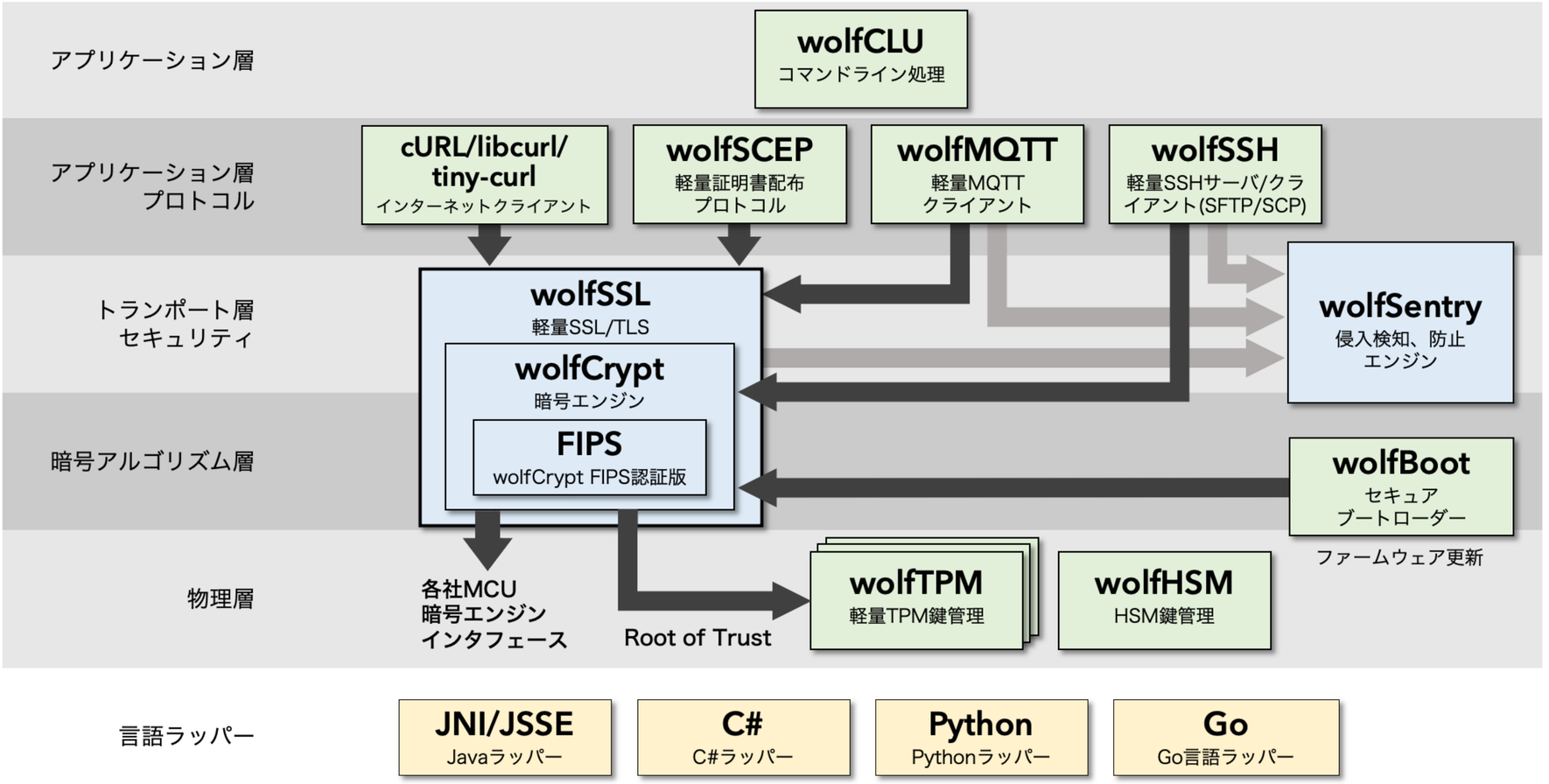
医療機器:
- 内視鏡検査装置
- 心電、生体センサ
- 介護モニター

自動車/鉄道関係:
- 車載AV
- エンジン制御
- 車両検査/計測機器
- 配車管理システム
- 信号システム

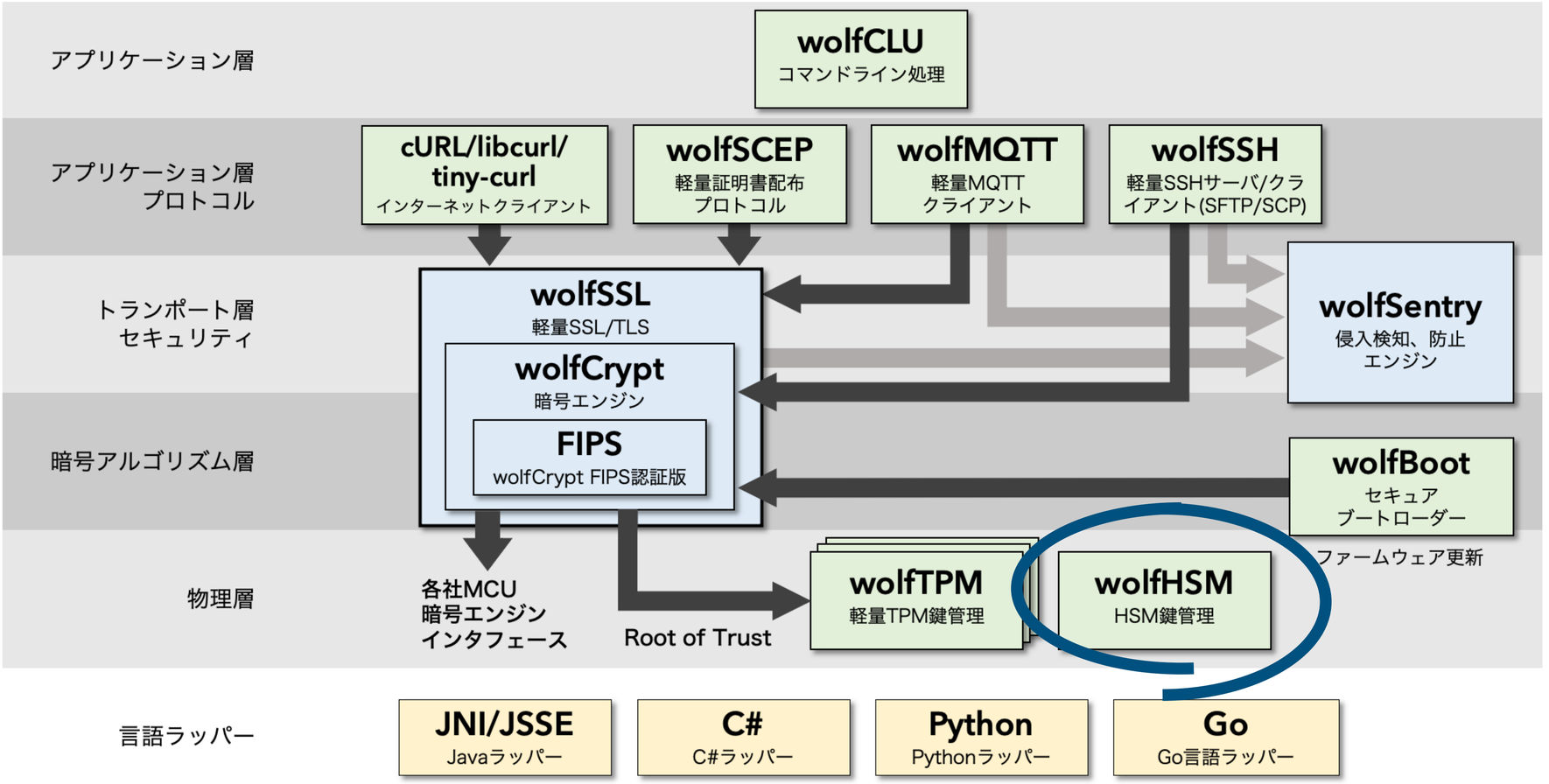
家庭/一般機器:
- デジタルカメラ
- 太陽光発電
- 健康機器
- スマートライト
- ドアホン/キー

写真はイメージです

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

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

HSM (Hardware Security Module) とは?

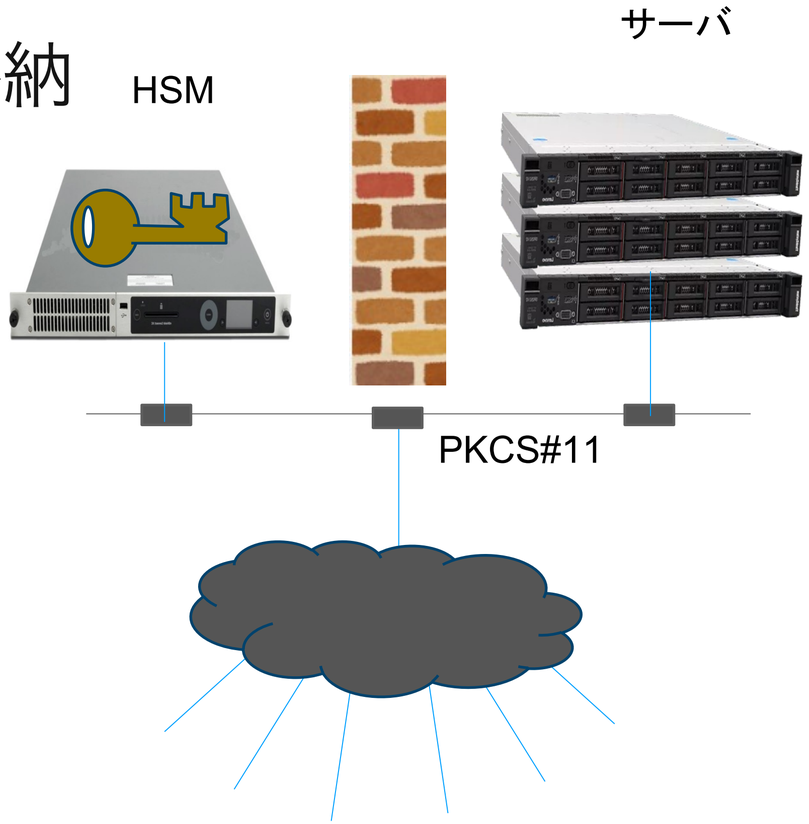
クラウドサーバとHSM

サーバ本体とは物理的に分離した筐体

秘密鍵などクリティカルなセキュリティ情報を格納

物理レベルの強固なセキュリティを実現

- 鍵管理
- 暗号・復号
- デジタル署名
- 認証
- セキュアブート、ファームウェアの保護
- アクセス制御



マルチコアMCUによるHSM

組み込み向け
マルチコアMCUで
Root of Trustを実現

車載向け：
ISO/SAE 21434/UN-R156
による実質的な義務化
(セキュアブートと
OTA: SOTA/FOTA)

HSMの利用シナリオ

セキュアブート、安全なファームウェア更新

- メジャードブート、コードの認証
- システム内アップデートとロールバック攻撃の検出

ネットワーク通信におけるデバイス認証

- OTA、V2X, V2Vなどの車両の認証
- プライベート鍵の生成、安全な鍵ストレージ
- 暗号化、ハッシュ、公開鍵署名アルゴリズム

キャリブレーション、構成データなどクリティカルデータの秘匿

HSMとTPM

HSM

TPMチップ

マイコン
チップ

TPM

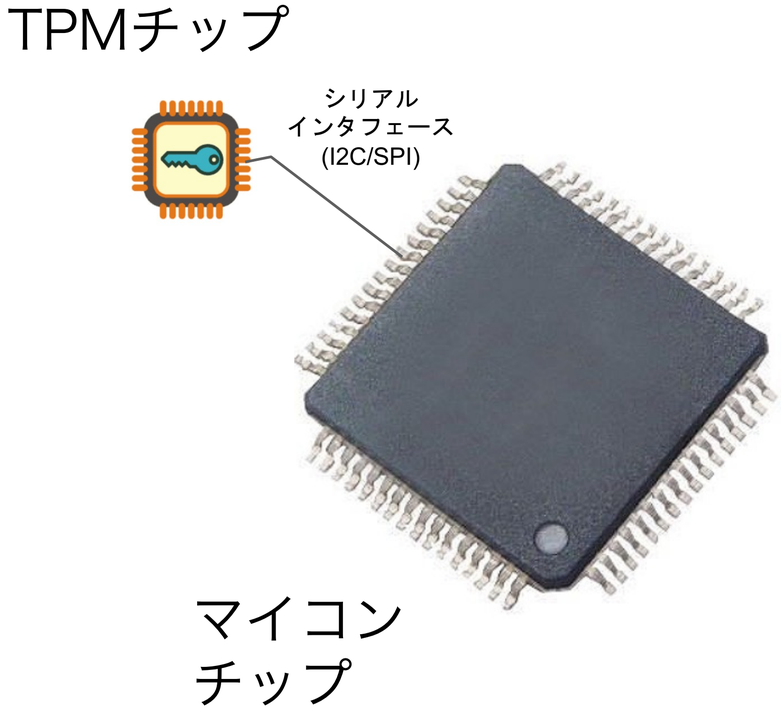
TPMとは

標準：TPM2.0（Trusted Platform Module 2.0）
TCG: Trusted Computing Group

シリアルインタフェースで接続された専用チップに
クリティカルなセキュリティ機能とデータを分離
ハードウェアベースの強固なセキュリティを実現

- 鍵生成と管理
- データ保護

- デバイスの認証
- セキュアブート
- プラットフォームの整合性検証
- ソフトウェアのライセンス保護



HSMとTPM

	HSM	TPM
標準化 (機能、I/F)	車載向け：AUTOSAR SHE+ HSMサーバ：PKCS#11	TPM2.0 TCG: Trusted Computing Group
拡張性	ハードウェア組み込み機能 ソフトウェア変更・拡張可	ハードウェア組込み機能 変更不可
接続	高速 オンチップバス	低速 オフチップ シリアルI/F(I2C, SIPなど)
暗号機能	乱数生成、署名検証、暗復号など	
	共通鍵暗復号、ハッシュなど 大量データ処理可	共通鍵暗復号など大量データ 処理には不向き

wolfHSMとは?

ソフトウェアによる暗号処理

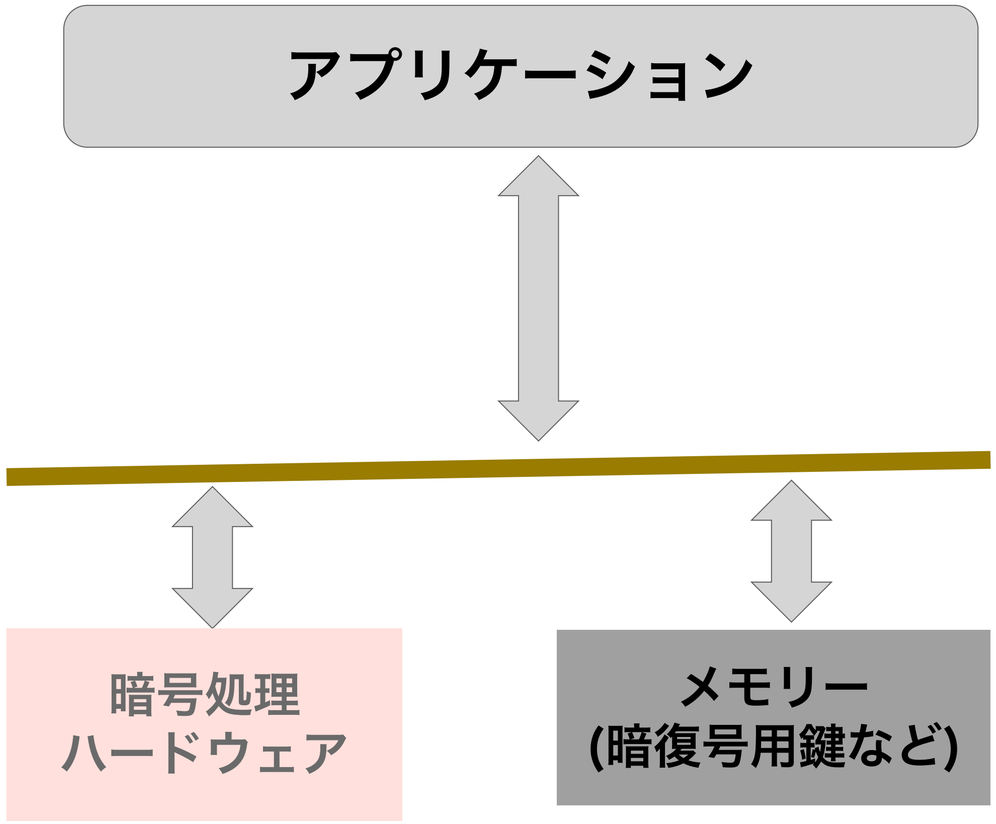
暗号処理：
- 鍵生成
- 暗復号
- 署名検証
- 乱数

アプリケーションコア

ハードウェアエンジンによる暗号処理

ハードウェア暗号処理：

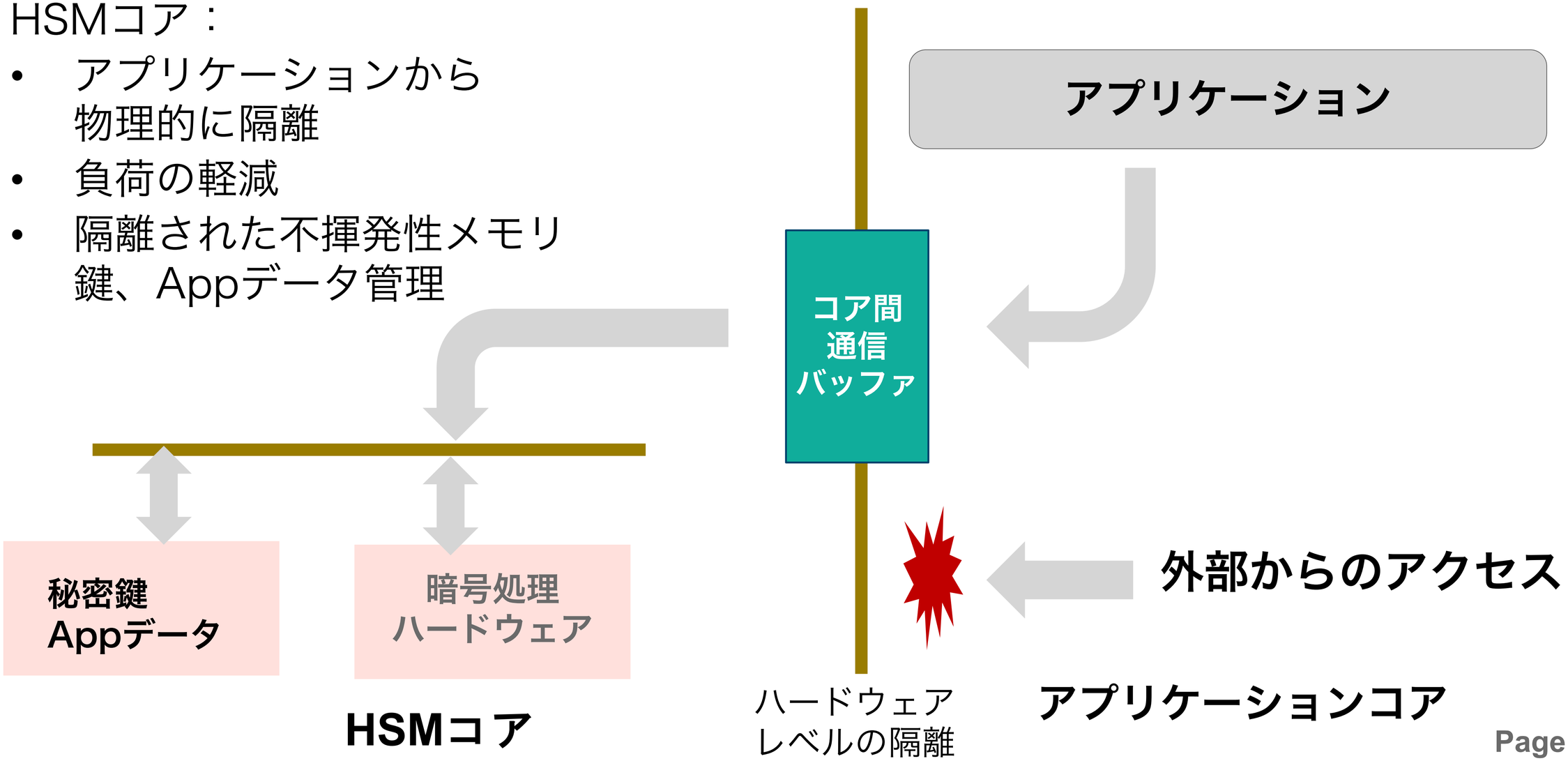
- 処理速度
- 負荷の軽減



チップベンダーによるHSM

HSMコア：

- アプリケーションから物理的に隔離
- 負荷の軽減
- 隔離された不揮発性メモリ鍵、Appデータ管理



wolfHSM

暗号アルゴリズム、機能の拡張性、柔軟性

暗号処理ソフトウェア

wolfCrypt
暗号処理
鍵管理
データ

秘密鍵
Appデータ

暗号処理
ハードウェア

HSMコア

コア間
通信
バッファ

アプリケーション

ハードウェア
レベルの隔離

アプリケーションコア

wolfHSMとセキュアブート

暗号アルゴリズム、機能の拡張性、柔軟性

暗号処理ソフトウェア

wolfCrypt
暗号処理
鍵管理
データ

ハッシュ
署名検証

署名検証
暗復号鍵

暗号処理
ハードウェア

HSMコア

コア間
通信
バッファ

ハードウェア
レベルの隔離

セキュアブート

wolfBoot

ハッシュ
署名検証

暗号化された
ファームウェア
イメージ

ハッシュ値
署名

アプリケーションコア

wolfHSMとセキュアブート

暗号アルゴリズム、機能の拡張性、柔軟性

暗号処理ソフトウェア

wolfCrypt
暗号処理
鍵管理
データ

ハッシュ
署名検証

NVM

署名検証
暗復号鍵

暗号処理
ハードウェア

HSMコア

コア間
通信
バッファ

ハードウェア
レベルの隔離

セキュアブート

wolfBoot

ハッシュ
署名検証
復号処理

暗号化された
ファームウェア
イメージ

ハッシュ値
署名

復号

ファームウェア
イメージ

アプリケーションコア

wolfHSMの基本機能

暗号アルゴリズム

- ハードウェア暗号の利用

  公開鍵、共通鍵、署名検証、乱数生成

  NVM(不揮発性メモリ)の利用
- 鍵管理
- データ管理

wolfHSMの基本機能

暗号アルゴリズム

- ハードウェア暗号の利用

  公開鍵、共通鍵、署名検証、乱数生成

  NVM(不揮発性メモリ)の利用
- 鍵管理
- データ管理

→ ソフトウェアによる機能拡張

wolfHSMの拡張性

暗号アルゴリズムの拡張

- ハードウェアベースのセキュリティを維持
  HSM専用コアで動作。HSM固有NVMに保存されたプライベート鍵
- 特定のハードウェア暗号アルゴリズム、鍵長などに限定されない
  公開鍵暗号、ECC曲線、鍵サイズ
- 領域固有：SM2, 3, 4
- **耐量子暗号:**

  Dilithium(ML-DSA), XMSS/XMSS^MT, LMS

量子コンピューティングの脅威と対策

- 既存の公開鍵暗号は、量子コンピューティングによって簡単に解読可能に

  → 既存**ハードウェア暗号エンジンの無力化**

- 耐量子暗号： 量子コンピューティングによっても解読が極めて難しい暗号アルゴリズム
- 耐量子暗号アルゴリズムへの移行が必須
  - 米CNSA2.0: 2030年までのロードマップ
  - 米NISTによるコンペティション(2016〜)、標準化(2024)

wolfCrypt

ハッシュ
SHA-2 (SHA-256, SHA-384, SHA512), SHA-3
(保守：MD2/5, SHA-1など)

共通鍵暗号
Camellia, AES (CBC, CTR, CCM, GCM, OFB), ChaCha20
(保守：3DES, ARC4, RABBIT, HC-128など)

公開鍵 鍵合意
RSA, DH, DHE, ECDH, ECDHE

公開鍵 署名
ECDSA, EdDSA(Ed25519/448), (保守：DSA)

楕円曲線サポート
NIST P-256他, Curve25519/448, Brainpool

メッセージ認証
HMAC, CMAC

パスワード認証
PBKDF2, PKCS#5

耐量子暗号
ML-KEM, ML-DSA, SLH-DSA
XMSS/XMSS^MT, LMS

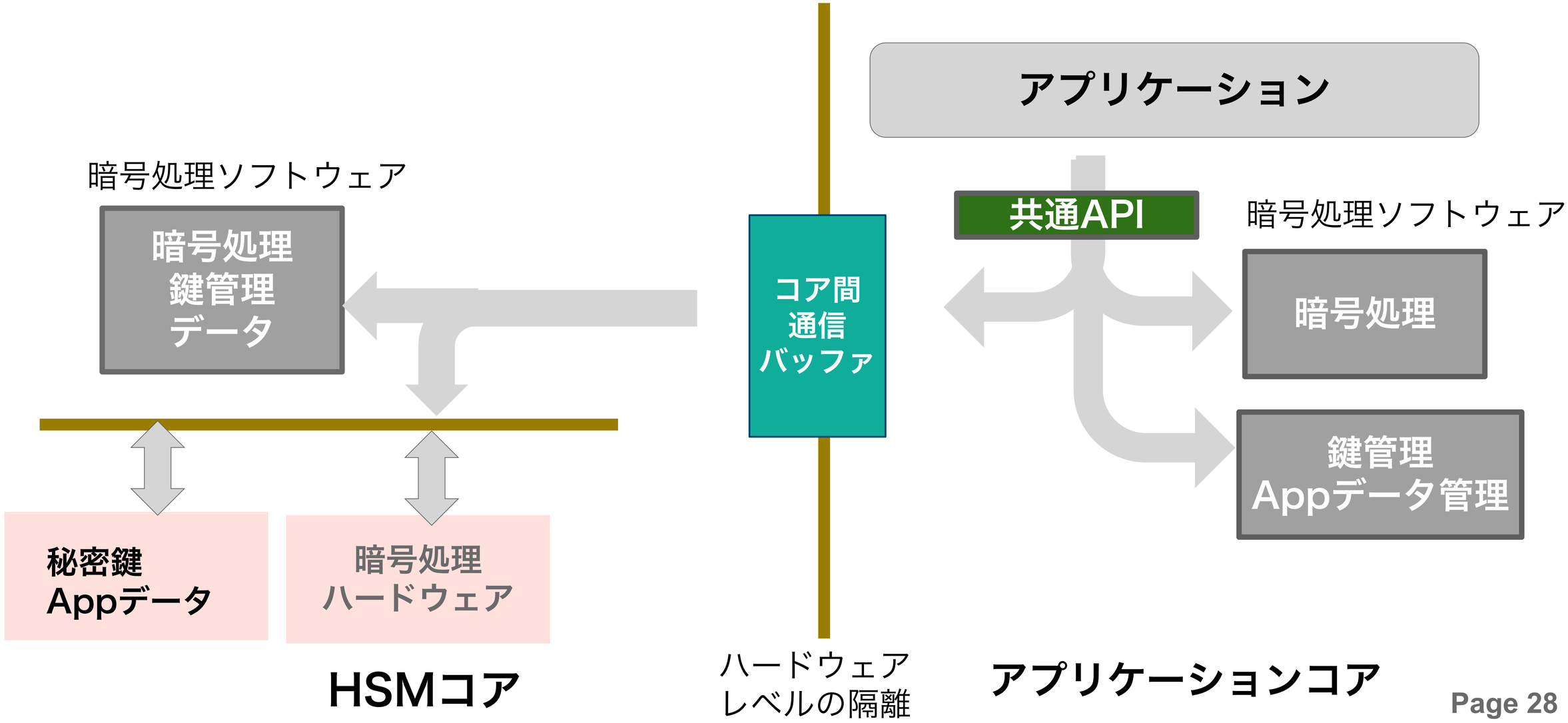
第三者認証
- FIPS140-3
  米国連邦政府の情報機器調達基準
- DO178-C
  航空機ソフトウェアの設計ガイドライン

wolfHSMと従来技術の親和性

共通API:

- アプリケーションコアのソフトウェア暗号処理
- HSMコアに隔離された
  - ハードウェア暗号処理
  - ソフトウェア暗号処理

共通API


アプリケーション
暗号処理ソフトウェア
暗号処理
鍵管理
データ
共通API
暗号処理ソフトウェア
コア間
通信
バッファ
暗号処理
鍵管理
Appデータ管理
秘密鍵
Appデータ
暗号処理
ハードウェア
HSMコア
ハードウェア
レベルの隔離
アプリケーションコア

インテグレーション

自社製品

- wolfBoot: 安全なファームウェア更新
- wolfSSL: デバイス認証
- wolfPKCS11: HSMの標準インタフェース (PKCS#11)

AUTOSAR

- 暗号処理、鍵管理、乱数生成
- セキュアブート、ソフトウェア更新

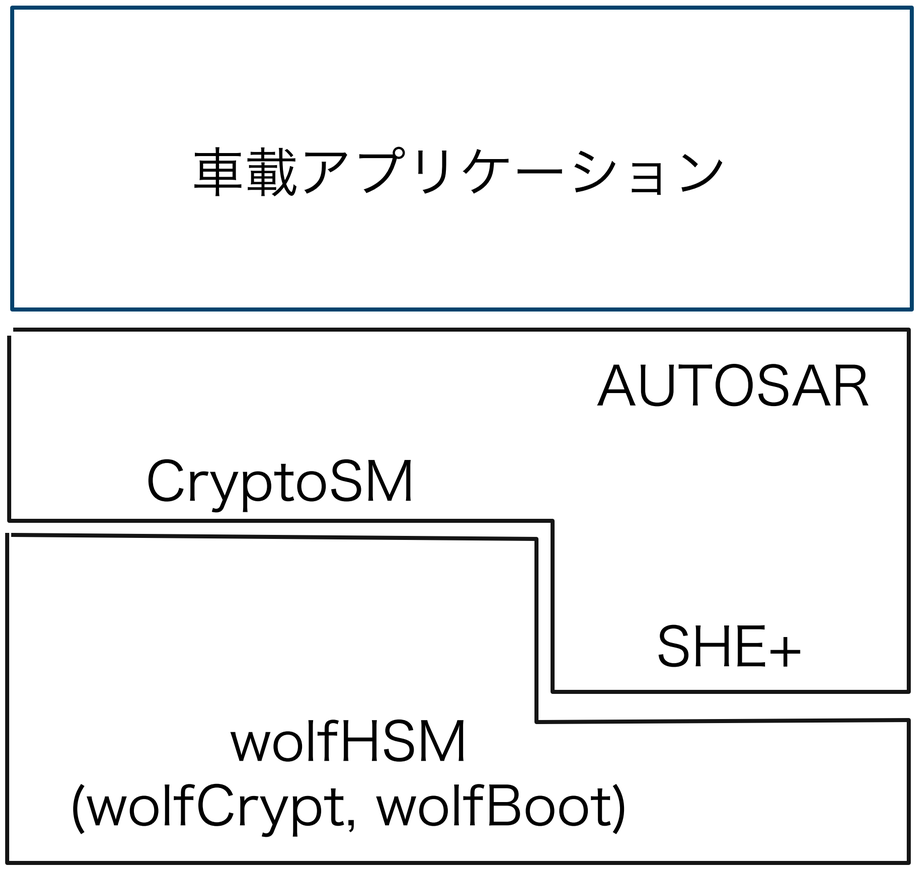
ソフトウェアベースのセキュリティ

CryptoSM (Crypto Service Manager)

ハードウェアベースのセキュリティ

SHE+（Secure Hardware Extension）

インテグレーション：AUTOSAR



wolfHSMの対応プラットフォーム

Infineon Aurix TC3xx

- 300MHz TriCoreアプリケーションコア：最大6コア
- 100MHz ARM Cortex M3 HSMコア
- HW暗号: TRNG, AES128, ECDSA, ED25519, SHA

ST SPC58NN

- 200MHz e200z4256 PowerPCアプリケーションコア：3コア
- 100MHz e200z0 PowerPC HSMコア + NVM
- HW暗号: TRNG, AES128

ルネサス RH850/F1K (開発中)

ソフトウェア、マニュアル

ソースコード：

ダウンロードページ： https://wolfssl.jp/download/

Github: https://github.com/wolfssl/wolfhsm

マニュアル

https://wolfssl.com/docs

wolfHSM

wolfHSM Manual	wolfHSM Manual (HTML)
wolfHSM Manual PDF	wolfHSM Manual (PDF)

テクニカルサポート

support@wolfssl.com

wolfSSLのRoot of Trust

製品名	標準	サポート	インタフェース
wolfTPM	TPM2.0/TCG	Infineon Optiga SLB9670 ST Micro ST33 Microchip ATTPM20 Nations Tech Z32H330 Nuvoton NPCT650	SPI/I2C/MMIO
wolfCrypt/PKCS11	PKCS #11	標準的なPKCS#11エンジン wolfPKCS11	Criptoki APIs
wolfSSL/IotSafe	IoT Safe/GSMA	SIM thru Serial Modem	UART
wolfHSM	ベンダー独自	Multi-core MCU Infineon Aurix TC3xx, TC4x ST SPC58NN	Shared memory
wolfCrypt/ セキュアエレメント	ベンダー独自	Microchip ATECC608 NXP SE050 STM STSAFE-A110 Maxim/Analog Devices MAXQ1065	SPI/I2C
wolfCrypt/ セキュアエンクレーブ	ベンダー独自	Arm TrustZone Intel SGX	Shared memory System Call
wolfSSL 鍵ラッピング	ベンダー独自	Renesas RX: TSIP, RA: SCE NXP iMX. CAAM Black Key	チップ内部バス

まとめ

HSMとは

wolfHSMとその特徴

- 柔軟性、拡張性
- 従来技術との親和性
- インテグレーション
- 製品実装

Q&A

info@wolfssl.jp