RZ Ecosystem Partner Solution

Tuxera 暗号ライブラリ HE-CRYPTO

国内販売代理店：株式会社ユビキタスAIコーポレーション

概要

MISRA Cに準拠し、高度な検証ツールによって検証済みの高信頼・高品質の組込み向け暗号ライブラリです。ユーザ／通信相手の認証、セキュアなデータの改ざん検知や保護等、RZファミリで利用可能です。またストレージ／ファイル単位の暗号化もHE-FILEと組み合わせて使用することにより可能となります。必要な暗号アルゴリズムのみを選択購入可能なため、低コストでセキュリティ機能を実現できます。

主な機能

- アメリカ国家安全保障局 NSA Suite B 対応
- 共通鍵・公開鍵暗号、電子署名、ハッシュアルゴリズム提供
- オープンソースやサードパーティコードを含まない完全オリジナルコード
- 暗号アクセラレータなどハードウェアなしで動作（ソフトウェア暗号ライブラリ）
- HCC独自のEEM（Embedded Encryption Module)により各種アルゴリズムは共通APIで利用可能
- 各種SoCに搭載された暗号アクセラレータを利用したライブラリも提供可能
- ソフトウェア暗号ライブラリ及び暗号アクセラレータライブラリは同一の共通APIで利用可能

ブロック図/ダイヤグラム

種別	機能	アルゴリズム
AES	暗号	AES-CBC / CFB / CTR / CCM / CCM8 / GCM / CMAC
Base64	エンコーダ	Base64
DSS	デジタル署名	DSS
ECC	鍵交換 / デジタル署名	ECDH / ECDHE / ECDSA
EDH	鍵交換	EDH
MD5	ハッシュ	MD4, MD5, MD5-HMAC
RSA	暗号 / 鍵交換 / デジタル署名	RSA, RSASSA-PSS
SHA	ハッシュ	SHA1, SHA2, SHA1-HMAC, SHA2-HMAC
TDES	暗号	DES, TDES-CBC / CBC-RAW
TIGER	ハッシュ	TIGER-128 / 160 / 192 / HMAC

ターゲット市場および用途

- HMI機器
- セキュリティ機器
- カメラデバイス
- FA機器
- 2D/3D表示機器
- スマートホーム
- 医療機器
- 車載機器
- エッジAI機器

https://www.ubiquitous-ai.com/products/he-crypt/

2021.10

Tuxera 社 ソリューションシリーズ

■ TCP/IP スタック　HE-NET

MISRA Cに準拠し高度な検証ツールによって検証済みの高信頼・高品質の組込み向けTCP/IPスタックです。TLS1.3やSSHなどセキュリティオプションも提供可能。高機能ARM MPU RZ ファミリを支援するネットワークコネクティビティを提供します。

■ USB スタック　HE-USB

USBホストスタック、USB デバイススタックを提供、豊富なクラスドライバにより RZ ファミリへ多様なUSBホスト／デバイス／OTG 機能を実現します。

■ FAT 互換ファイルシステム　HE-FILE

RZファミリで利用する、SD、eMMC、USB、Raw Flashデバイスに対して、FAT、exFAT互換ファイルシステム機能を提供します。
リムーバブルメディアの場合、PC、Macとの相互のファイルデータ交換を実現します。
更に、耐電源断機能を持つセーフティファイルシステムも提供可能です。

お問い合わせ

株式会社ユビキタスAIコーポレーション

https://www.ubiquitous-ai.com/

E-mail:sales@ubiquitous-ai.com

本　社	〒160-0023	東京都新宿区西新宿1-21-1 明宝ビル6F	TEL 03-5908-3451	FAX 03-5908-3452
五反田	〒141-0031	東京都品川区西五反田2-25-2 飯嶋ビル	TEL 03-3493-7981	FAX 03-3493-7993
大　坂	〒532-0011	大阪府大阪市淀川区西中島6-2-3 1205	TEL 06-6304-5700	FAX 06-6304-5705
名古屋	〒460-0008	愛知県名古屋市中区栄5-19-31 T&Mビル	TEL 052-262-6451	FAX 052-262-6460