RA Ecosystem Partner Solution

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。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

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
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

- IoTデバイス
- セキュリティ機器
- 産業機器
- FA機器
- ウェアラブルデバイス
- 家電
- 医療機器
- 車載機器
- 事務機器

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

2021.09

HCC Embedded 社 ソリューションシリーズ

■ TCP/IP スタック　HE-NET

MISRA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なため RA ファミリを利用したセキュアなIoTシステムに最適です。

■ 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 RA ファミリへ多様な USB 機能を実現します。組込み向けに最適化されたスタックは少ない ROM/RAM サイズのため RA ファミリを利用した IoT システムに最適です。

■ FAT 互換ファイルシステム　HE-FILE

ワンチップマイコンでの使用を前提に少ない ROM/RAM サイズで動作するよう設計され、各RTOS環境やOSがない環境で動作が可能です。さらにリソースが厳しいプロジェクト向けの超省RAM製品、電源断対応製品、exFAT互換製品など、多様なファイルシステム製品を提供します。

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