TUXERA
Make it work.

Ubiquitous AI

RL78 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

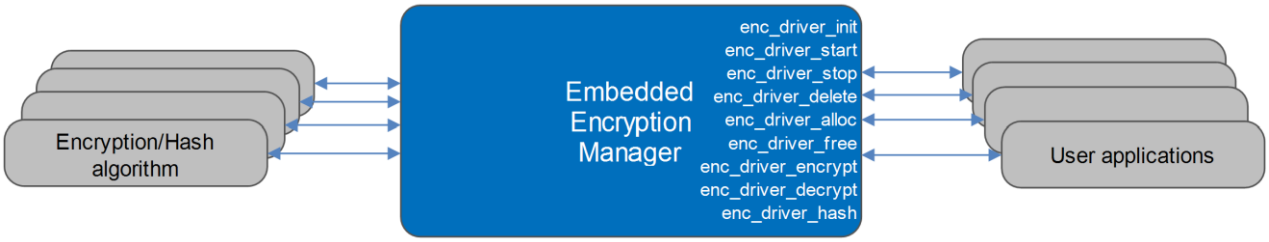
概要

HE-CRYPTOはMISRAに準拠し、厳しい開発プロセスを経て開発された高信頼・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だけを選択して購入できるので、新規製品はもちろんのこと、既存製品に後付けでセキュア機能を追加することが可能です。暗号化・改ざん検知・認証などのセキュリティ機能を、低コストで実装できます。16ビットマイコンや小ROM/RAMサイズマイコンで動作するように設計されており、RL78ファミリに適した暗号化ライブラリです。日本国内でのお問い合わせは株式会社ユビキタスAIまで。

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、デジタル署名、ハッシュアルゴリズム提供
- データ暗号化、改ざん検知、認証処理が可能
- 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
- ソースコード提供（MISRA C準拠）
- 高速な多倍長演算処理を搭載

ブロック図 / ダイヤグラム



ターゲット市場 / 用途

- IoTデバイス
- 車載機器
- ウェアラブルデバイス
- 医療機器
- 産業機器
- FA機器
- 家電
- 事務機器

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

2023.09

TUXERA
Make it work.

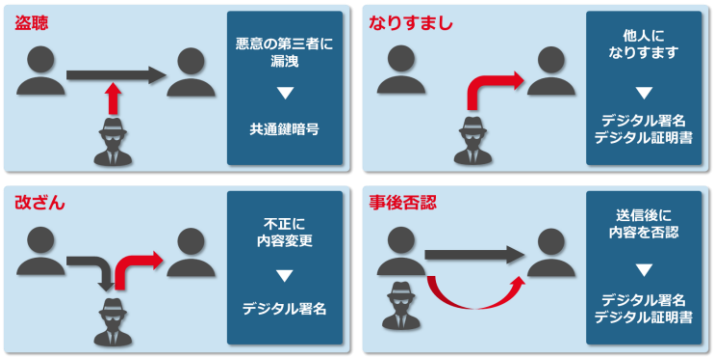
Ubiquitous AI

RL78をセキュリティ対応化するソフトウェア暗号ライブラリ

HE-CRYTO

制御システム向けIEC62443や車載向けUN-R155/156などのサイバーセキュリティ要件への対応が求められ、データ/プログラム改ざん、デバイスなりすまし、データ盗聴などの脅威から機器を守ることが必須になってきています。

■ データ通信時の脅威と対処



共通鍵暗号：AES

デジタル署名：ECDSA+SHA, RSA+SHA

ハッシュ：SHA, MD5

など

■ サポートアルゴリズム

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
ChaCha20	暗号	ChaCha20
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

ROM/RAMサイズは、コンフィグレーションにより調整が可能です。サイズが厳しい環境向けには、メーカーによるカスタマイズも可能ですので、是非ご相談ください

お問い合わせ

株式会社ユビキタスAI www.ubiquitous-ai.com E-mail:sales@ubiquitous-ai.com

本　社 〒160-0023 東京都新宿区西新宿1-23-7 新宿ファーストウエスト17F TEL 03-5908-3451
大　坂 〒532-0011 大阪府大阪市淀川区西中島6-2-3 1205 TEL 06-6304-5700
名古屋 〒460-0008 愛知県名古屋市中区栄5-19-31 T&Mビル 3F-F TEL 052-262-6451

Tuxera www.tuxera.com

Global HQ Westendintie 1, 02160 Espoo, Finland TEL +358-20-764-1720
Tuxera USA 2118 20th Avenue SE, Suite 135 Bothell, WA 98021 TEL +1-800-221-6630.
Tuxera Hungary Vaci ut 76, Budapest H-1133
Tuxera Japan 3-7-1 Minatomirai, Nishi-ku, Yokohama-Shi, Kanagawa, 220-0012