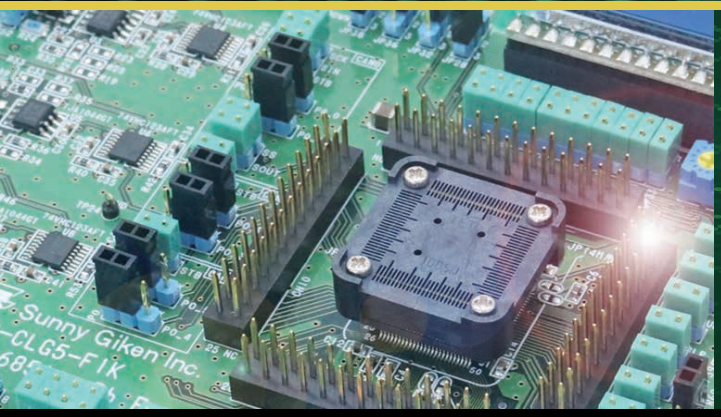
株式会社サニー技研

RH850 車載用マイコン Security Support

ルネサスエレクトロニクス 32bit マイコン RH850 シリーズのセキュリティ開発支援

マイコン内蔵 HSM（ハードウェアセキュリティモジュール）の導入・開発立ち上げを
サポートする技術支援を行います。
レクチャー、QA サポート、動作環境の立ち上げサポートまで、
ユーザー状況に合わせたサポートをご提供します。

サポート対応マイコン



- RH850/F1KM-S1
- RH850/F1KM-S4
- RH850/U2A

ユーザーが使用するマイコンに合わせて対応します。

セキュリティ導入教育

セキュリティ開発を始めるにあたって必要となるセキュリティ技術をレクチャーします。
ユーザーが使用するマイコンに合わせた内容のため、すぐに応用できる実践的なノウハウを学べます。

コース	概要	レクチャー項目	NDA※
セキュリティ導入教育（初級編）	セキュリティ初心者の方を対象とした導入教育です。 セキュリティで何を守ろうとしているのか、 その仕組みなどを暗号技術を中心に基礎から説明します。	・セキュリティ用語説明 ・自動車への脅威 ・ブロック暗号 ・ハッシュ関数 ・Root of trust	不要
セキュリティ導入教育（HSM 編）	ユーザーが使用するマイコン内蔵の HSM の概要を説明し、 セキュリティの開発環境の準備から HSM の使い方などを レクチャーします。	・HSM 初期化 ・HSM デバッグ方法 ・Secure boot ・Secure boot の分割と高速化 ・Application と Security の役割分担 ・DataFlash の排他処理	必要
セキュリティ実習	実習形式で HSM の使い方を身につけることができます。 ユーザーが使用するマイコン内蔵 HSM に合わせた セキュリティスターターキットを用いて実習します。	・HSM 初期化 ・HSM デバッグ方法 ・乱数の生成 ・鍵登録 ・CMAC 生成 / 検証 ・Secure boot	必要

※セキュリティ情報を取り扱いますので、ユーザーとルネサスエレクトロニクスとの NDA 締結を前提とします。

セキュリティ技術支援

HSM の使い方を対象とした ECU サポートです。
ユーザーの開発中での HSM 不明点やセキュリティ仕様のレビューを実施します。

RH850 マイコン内蔵 HSM の動作検証環境

Security Starter Kit

HSM 導入ソフト（Hello World）で HSM 動作がすぐに試せるスタータキットです。
実際に動かしながらセキュリティサービスの動作理解や処理時間の計測が可能です。
ECU 開発立ち上げ時のリファレンスとしても、ご利用できます。

マイコン内蔵 HSM を使う時の課題

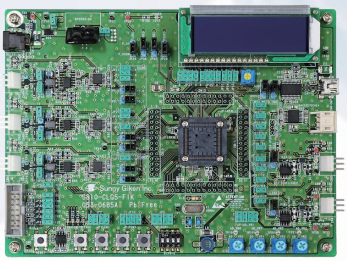
マイコンに内蔵されている HSM 機能を使おうとして困ったことはありませんか？
HSM のアーキテクチャ検討、初期性能検証時の課題は数多くあります。

初期検討課題

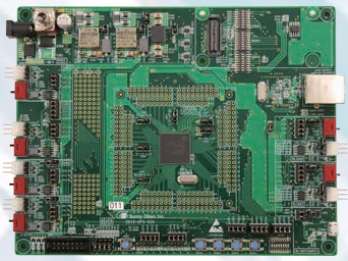
- 鍵の登録 / 運用方法を検討したい
- HSM を使った暗号化 / 復号の処理時間を計測したい
- セキュアブートにかかる時間を計測したい
- SecOC の MAC 値演算の処理時間を調べたい

ユーザーの課題

- HSM の仕様がわからないので立ち上げがうまく出来ない
- HSM の鍵の登録ができない
- セキュアブートが出来ない
- HSM 用 Firmware の開発が出来ない

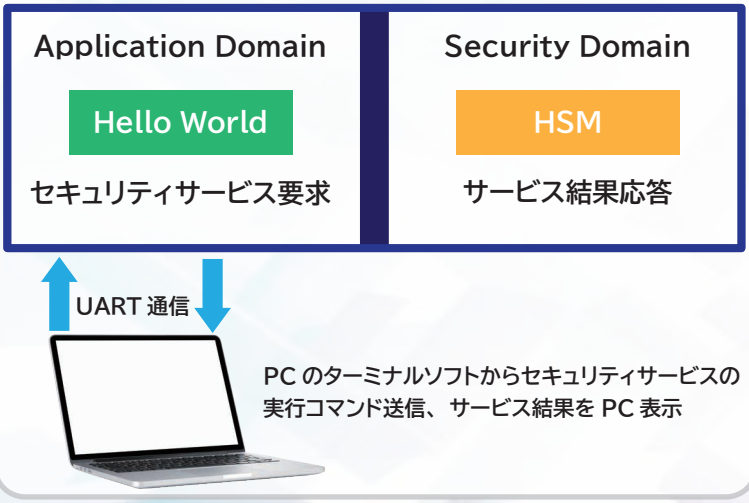


RH850/F1KM-Sx 対応
評価ボード



RH850/U2A 対応
評価ボード

MCU 内部イメージ



PC のターミナルソフトからセキュリティサービスの
実行コマンド送信、サービス結果を PC 表示

Security Starter Kit ラインナップ

マイコン評価ボードと HSM 導入ソフトをセットで提供

製品名	対応マイコン
EVITA-Light セキュリティスタータキット	RH850/F1KM-S1
EVITA-Medium セキュリティスタータキット	RH850/F1KM-S4
EVITA-Full セキュリティスタータキット	RH850/U2A

マイコンに合わせた ICU-S ドライバ、ICU-M ファームウェアは、
ユーザーがルネサスエレクトロニクスから取得するものとします。[*]

HSM 導入ソフト（Hello World）を同梱

1. HSM のセキュリティサービスを実行

（1）内蔵乱数生成器を用いた乱数生成
（2）SHE に準拠した NVM 鍵登録
（3）NIST SP800-38B CMAC を用いた CMAC 生成 / 検証
（4）NIST SP800-38A ECB/CBC 暗号化 / 復号

その他、HSM ドライバやファームウェアが提供している
セキュリティサービスに対応しています。

2. PC から HSM のセキュリティサービスを実行

PC のターミナルソフトから各セキュリティサービスの実行とともに
処理時間の計測が可能です。

[*] セキュリティ情報を取り扱いますので、ユーザーとルネサスエレクトロニクスとの NDA が必要となります。

【お問合わせ】
株式会社サニー技研　名古屋事業所
〒460-0003　愛知県名古屋市中区錦 2-2-13 名古屋センタービル本館 5F
TEL：052-221-7600（代表）/ FAX：052-221-0071
MAIL：info@sunnygiken.co.jp / URL：https://sunnygiken.jp

【サニー技研 車載セキュリティ技術情報ページ】
https://sunnygiken.jp/innovation/automotive-security/

2022 年 9 月発行