|  |
| --- |
| AN229503 |
| Semper Secure NORフラッシュのRMA用セットアップ

|  |
| --- |
| 著者：Zhi Feng |
| 関連するパーツファミリ：S35HL-T / S35HS-TS36HL-T / S36HS-TS38HL-T / S38HS-T |

  |
| このアプリケーションノートでは、サイプレス Semper™ Secure NORフラッシュメモリをRMAライフサイクルステージにセットアップする手順について説明し、ホストアプリケーションソフトウェアを実装するためのガイドラインと提案を提供します。 |

# はじめに

Semper Secure NORフラッシュデバイスは、図1に示すように、いくつかの段階を含む単方向のライフサイクルに従います。デバイスは秘密を保存せずにNOMALライフサイクルステージで出荷されます。その後、さまざまなライフサイクルステージを移動できます。PROVISIONライフサイクルステージで、ユーザーはフラッシュデバイスを対応するMCUホストとペアリングし、セキュアリージョン構成と必要なキーをセットアップします。デバイスがフィールドで使用されるとき、SECUREライフサイクルステージです。ユーザーが障害分析のためにデバイスをサイプレスへ返却する必要があるシナリオの可能性を期待している場合は、返品承認（RMA）の準備をする必要があります。RMAライフサイクルステージにより、サイプレスはフィールドの問題を分析するためのテストを実行できます。

このドキュメントではRMAオプションを準備し、デバイスをSECUREステージからRMAステージに移行する手順について説明します。ユーザーはすでにSemper Secureのデータシートと標準操作に精通していることを前提としています。操作の詳細はこのドキュメントでは繰り返されていませんが、対応するデータシートに記載されています。このドキュメントに記載されているAPI（*イタリック体*）の詳細についてはデータシートを参照してください。

このドキュメントでは特に指定がない限り、”デバイス”を使用してSemper Secureフラッシュデバイスを指し、”ホスト”を使用してペアのホストMCUを指します。*イタリック体*の単語はSemper Solution Development Kit（S-SDK）で使用できるAPI関数を示します。

図1. Semper Secure NOR フラッシュライフサイクル



# RMAの準備

## オプションを決定する

Semper Secureデバイスを最初に受け取ったときに、将来的にRMAライフサイクルを許可するかどうかを決定する必要があります。ホストとの最初のペアリング時に、*SetInitialConfig*トランザクションを介してそのようなオプションをデバイスにプロビジョニングします。デバイスがプロビジョニングされると、オプションを変更することはできません。したがって、将来的に障害分析が必要になる可能性がある場合、将来的にRMAライフサイクルステージに移行できるようにデバイスをプロビジョニングする必要があります。

*SetInitialConfig*トランザクションはデータシートで定義されているデバイス構成パラメーターが必要です。パラメーターの1つは”RMA対応”です。RMAオプションが許可されている場合、このフィールドは’1’に設定する必要があります。それ以外の場合は’0’を入力する必要があります。同じパラメータテーブル内のフィールド”RMAキーインデックス”はキーストレージ領域内にRMAキーを保存するインデックスを指定します。サイプレスは値’65’の使用を提案しています。RMAインデックスがマスターキーインデックスと異なる限り、65から99までの任意の値を選択できることに注意してください。

データシートの*SetInitialConfig*コマンドセクションを参照してください。

## RMAキーを設定する

RMAを許可するオプションを選択した場合、フィールドでデバイスを使用する前にRMAキーをデバイスにプログラムしてください。これは*ProgramKey*トランザクションで実行されます。

非対称デバイスの場合、ホストはRMA公開キーをデバイスにプログラムする必要があります。対称デバイスの場合、共有RMA秘密キーは暗号化を使用してデバイスにプログラムする必要があります。*ProgramKey*トランザクションの形式を以下に示します。

***ProgramKey*書き込みパケット**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CMDコード | アドレス | 索引 | 分類 | サイズ | Nonce | データ: | TAGまたはMAC |
| 2バイト | 1バイト | 1バイト | 2バイト | 2バイト | 16バイト | 最大512バイト | 16バイトまたは32バイト |
| [0:1] | [2] | [3] | [4:5] | [6:7] | [8:23] | [24:43] | [44:size+23] | [size+24:size+55] |
| 0040h | address = 00h | index = 41h | type = 0001h | データのサイズ | nonce | security\_parameters | encrypted\_key\_valueまたはplain\_key\_value | tagまたはmac |
| 非対称デバイス：RMA公開キー（key\_valueの暗号化なし）mac = HMAC (master\_session\_key, CMD\_Code||Address||index||type||size||nonce||security\_parameters||plain\_key\_value||(++CMD\_Counter))対称デバイス：RMA秘密キー（AES-GCMによって暗号化されたkey\_value）GCM\_Counter = lower 32-bit (++CMD\_Counter)GCM\_IV = lower 64-bit (master\_session\_key) || GCM\_CounterAAD = CMD\_Code || address || index || type || size || nonce || security\_parametersencrypted\_key\_value, TAG = AES-GCM(master\_session\_key, GCM\_IV, AAD, plain\_key\_value) |

***ProgramKey*応答パケット**

|  |  |  |
| --- | --- | --- |
| 対応 | 結果 | MAC |
| 2バイト | 2バイト | 32バイト |
| [0:1] | [2:3] | [4:35] |
| 4000h | 結果 | mac |
| mac = HMAC(master\_session\_key, response||result||(++CMD\_Counter)) |

# RMAへの移行

## 機密データを破棄する

障害分析のためにSemper Secure NORフラッシュデバイスを返却することを決定した後、デバイスをRMAライフサイクルステージに移行する前に、デバイス上の機密データを消去するのはユーザーの責任です。デバイスがRMAに入ると、安全なトランザクションを実行するためのセッションキーを確立できなくなります。

安全なリージョン内のデータを削除するには、リージョンのアクセスレベルに応じて消去オプションを実行します。例えば、*AuthenticatedErase*または*EncryptedErase*トランザクションを使用します。

すべてのキーは暗号化された形式で保存され、暗号化キーはRMAライフサイクル段階でハードウェア保護ではアクセスできないUnique Device Secret（UDS）から取得されるため、キーストレージ領域内のキーを削除する必要はありません。

## RMAセッションキーを設定する

デバイスをRMAに移行する前に、ホストはRMAセッションキーを確立する必要があります。これは*CreateSesionKey*と*StoreSessionKey*の2段階のトランザクションによって実行されます。このトランザクションは、マスターセッションキーまたはリージョンセッションキーの作成と同じ方法に従います。これはすべてのセキュアトランザクションがSECUREライフサイクルステージ中にセッションキーを必要とするため、よく知っている必要があります。

非対称デバイスの場合、RMAセッションキーを生成するにはデバイスにすでにプログラムされているRMA公開キーが必要です（RMAキーの設定を参照）。ホストはデバイスからエイリアス公開キーも取得している必要があります。これはエイリアス公開キー情報を含むエイリアス証明書を読み取ることで実行できます。

対称デバイスの場合、RMAセッションキーを生成するにはMCUホストとデバイスの両方が、共有RMA秘密キーを知っている必要があります。この秘密キーはすでにデバイスにプログラムされている必要があります（RMAキーの設定を参照）。

必要なキーが配置されている場合は、*CreateSessionKey*コマンドと*StoreSessionKey*コマンドを発行して、RMAセッションキーを確立できます。詳細については、データシートの*CreateSessionKey / StoreSessionKey*セクションを参照してください。*CreateSessionKey*および*StoreSessionKey*トランザクションパケットの形式を以下に示します。

***CreateSessionKey* 書き込みパケット**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CMDコード | アドレス | 分類 | Nonce | セキュリティパラメータ | CRC-16 |
| 2バイト | 4バイト | 2バイト | 16バイト | 20バイト | 2バイト |
| [0:1] | [2:5] | [6:7] | [8:23] | [24:43] | [44:45] |
| 000Ah | Address = 00000000h | type = 0002h | nonce\_u | security\_parameters | crc\_checksum |

***CreateSessionKey*読み取りパケット**

|  |  |  |  |
| --- | --- | --- | --- |
| 対応 | 結果 | Nonce | MAC |
| 2バイト | 2バイト | 16バイト | 32バイト |
| [0:1] | [2:3] | [4:19] | [20:51] |
| 0A00h | 結果 | nonce\_v | mac |
| mac = HMAC(new\_session\_key, response||result||nonce\_v||(++CMD\_Counter)) |
|  |

***StoreSessionKey*書き込みパケット**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CMDコード | アドレス | 分類 | データ: | MAC |
| 2バイト | 4バイト | 2バイト | 32バイト | 32バイト |
| [0:1] | [2:5] | [6:7] | [8:39] | [40:71] |
| 001Eh | address = 00000000h | type = 0002h | MacTagU | mac |
| 非対称デバイスの場合：MacTagU = HMAC（new\_session\_key、 "KC\_1\_U" || pub\_key\_u || pub\_key\_v || nonce\_u || nonce\_v）;ここで、pub\_key\_uとpub\_key\_vは、それぞれホスト側とデバイス側でnew\_session\_keyを導出するために使用される公開キーです。mac = HMAC(new\_session\_key, CMD\_Code||address||type||MacTagU||(++CMD\_Counter))対称デバイスの場合：MacTagU = HMAC(new\_session\_key, nonce\_v||nonce\_u)mac = HMAC(new\_session\_key, CMD\_Code||address||type||MacTagU||(++CMD\_Counter)) |

***StoreSessionKey*読み取りパケット**

|  |  |  |
| --- | --- | --- |
| 対応 | 結果 | MAC |
| 2バイト | 2バイト | 32バイト |
| [0:1] | [2:3] | [4:35] |
| 1E00h | 結果 | mac |
| mac = HMAC(new\_session\_key, response||result||(++CMD\_Counter)) |

## *TransitionToRMA*トランザクションを実行します

RMAセッションキーが確立されたのち、*TransitionToRMA*トランザクションを発行してデバイスをRMAライフサイクルステージに移動できます。

***TransitionToRMA*書き込みパケット**

|  |  |  |
| --- | --- | --- |
| CMDコード | 予約済み | MAC |
| 2バイト | 2バイト | 32バイト |
| [0:1] | [2:3] | [4:35] |
| 0030h | 0000h | mac |
| mac = HMAC(rma\_session\_key, CMD\_Code||Reserved||(++CMD\_Counter)) |

***TransitionToRMA*読み取りパケット**

|  |  |  |
| --- | --- | --- |
| 対応 | 結果 | MAC |
| 2バイト | 2バイト | 32バイト |
| [0:1] | [2:3] | [4:35] |
| 3000h | 結果 | mac |
| mac = HMAC(rma\_session\_key, response||result||(++CMD\_Counter)) |

*TransitionRMA*トランザクションが完了したら、障害分析のためにデバイスをサイプレスに返送できます。

# Semper SolutionSDKの使用

Cypress Semperソリューション開発キット（S-SDK）は、お客様が独自のドライバーを開発したり、提供されたコード例を直接使用したりできるように設計されたソフトウェアパッケージです。RMAへの移行はS-SDKが提供する例の1つです。S-SDKコードの例に従うか、プラットフォームに依存しないCコードを使用して、このドキュメントに記載されているこれらの手順を実行できます。

# 結論

障害分析のためにSemper Secure NORフラッシュデバイスをサイプレスに戻すには、事前の計画、RMAキーのインストール、機密データの保護、およびデバイスをRMAライフサイクルステージに移行するための実際の手順が必要です。このドキュメントでは、デバイスをサイプレスに返送する前に実行する必要のある手順をまとめています。ソフトウェア開発者は、このようなニーズが発生した場合に備えて、これらの手順に従ってソフトウェアを準備できます。

# 参考文献

002-26101 S35HS-T、S35HL-TSemperセキュアフラッシュとクアッドSPIデータシート

002-28332 AN228332 – Cypress Semper SecureNORフラッシュでの初期プロビジョニング

改訂履歴

＜＜★Document Number: 002-29503

| **版** | **Engineering Change Notification (技術変更届)** | **日付** | **変更内容** |
| --- | --- | --- | --- |
|  |  |  |  |