AN13483

SE050E - ユーザー・ガイドライン

Rev. 1.2 — 2022年8月22日　　アプリケーション・ノート

ドキュメント情報

情報	内容
キーワード	セキュア・エレメント, SE050E, ユーザー・ガイドライン, Plug & Trust, EdgeLock SE050E
概要	このドキュメントでは、新世代のSE050製品、SE050Eのユーザービリティとセキュリティに関する推奨事項を、ガイドラインとして提供します。このガイダンスは、IoTアプレット・バージョン7.2.0に対して有効です。

改訂履歴

改訂履歴：SE050E

Rev	日付	説明
1.2	2022年8月22日	• セクション7.2.5を更新 • 暗号処理ECDAAを削除
1.1	2022年5月25日	• セクション4.1を更新
1.0	2022年3月11日	初版

1　はじめに

このドキュメントには、システム・インテグレータとアプリケーション開発者向けに、EdgeLock SE050Eセキュリティ・モジュールの機能とセキュリティに関する推奨事項を記載しています。推奨事項の目的は、その推奨事項に従って通常の条件下で製品が使用されることを前提に、セキュアなソリューションを開発することです。

このドキュメントで言及しているのはSE05xのEdgeLock Ready構成、具体的にはSE050Eですが、これらの推奨事項はEdgeLock SE05xのカスタム構成にも適用されます（セクション6.2を参照）。

シングルテナントで使用する場合とマルチテナントで使用する場合では、違いがあります。

- **シングルテナント**は、SE050Eが異なるユーザーに対して個別に認証情報を保護しないことを意味します。認証情報を使用する際に、SE050Eでユーザーを区別する必要はありません。
- **マルチテナント**は、SE050Eがシークレット（認証オブジェクト）に基づき認証情報へのアクセスを区別することを意味します。マルチテナントは複数のユーザー（実際の利用者）で構成できますが、複数の異なるアプリケーションや、同じアプリケーションの複数のスレッドでも構成できます。

このドキュメントのシングルテナントに関するガイドラインは、SE050Eをシングルテナントで使用する場合にもマルチテナントで使用する場合にも常に適用できます。マルチテナントでの使用に特化したガイドラインは、シングルテナントでの使用には適用されません。

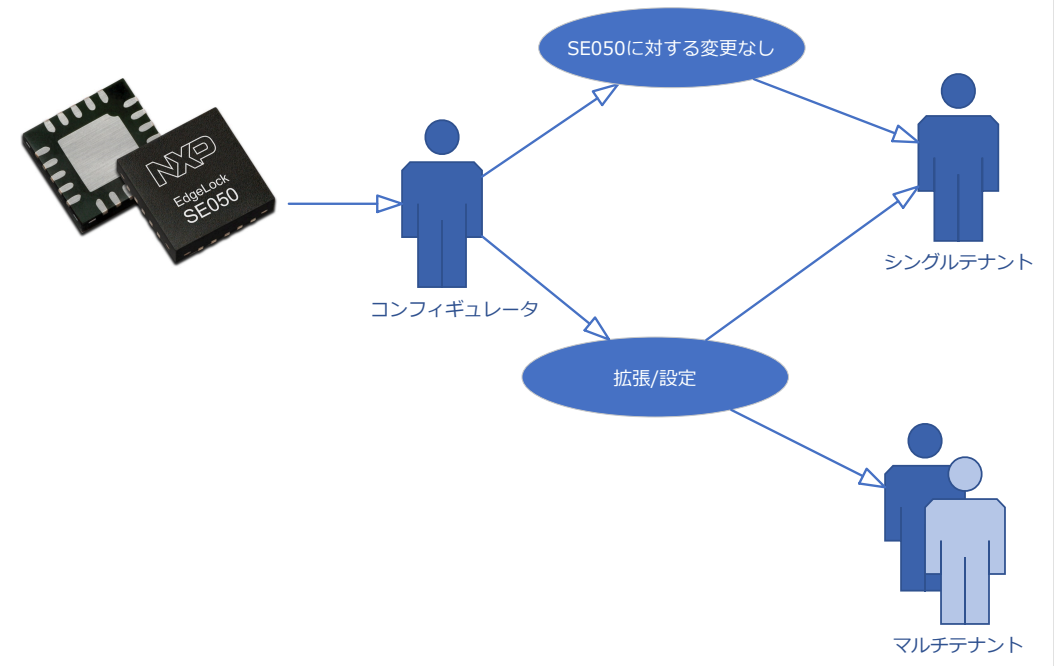

図1.シングルテナントとマルチテナント

以下の各章では、SE050Eのさまざまな使用方法について説明します。

- **SE050Eの基礎**
  - SE050Eの基礎として、セキュア・オブジェクトとはどのようなもので、どのように使用すればよいのかを説明します。
- **SE050E Plug & Trust：標準設定で使用**（シングルテナントとしてそのまま使用）
  - SE050Eセキュリティ・モジュールを、SE050Eを使用する単一のエンティティによって標準設定ですぐに使用する方法について説明します。各種の既製品で実行可能なユース・ケースについての一般的なガイドラインを提供します。

  - **Ease of Use設定**では、Plug & Trustに対応した今後市場で提供予定の汎用SE050E製品について説明します。これらのデバイスには、NXPによってトラスト・プロビジョニングされた特定の認証情報セットが付属します。
  - **シングルテナントのユース・ケース** では、SE050Eをシングルテナントで使用する場合に適用できる最もシンプルなユース・ケースについて説明します。この場合のシングルテナントとは、SE050Eが単一のインスタンスで操作されることを意味します。

- **SE050E Plug & Trust : 拡張性**（SE050Eを設定）
  - 新しくプロビジョニングした認証情報でEase of Use設定を拡張するユーザーやシステム・インテグレータ向けにサポートを提供します。これはシングルテナントで使用する場合（Ease of Use設定の他に認証情報を追加する場合など）にもマルチテナントで使用する場合（2人の異なるエンド・ユーザーが使用できるようにSE050Eを設定する場合など）にも適用できます。
- **SE050E Plug & Trust : マルチテナントで使用**
  - SE050Eセキュリティ・モジュールを複数のエンティティで使用する方法について説明します。ターンキー製品で実行可能なユース・ケースについての一般的なガイドラインを提供します。
  - **モジュールの説明（上級）**
    - セキュア・オブジェクト（上級）
    - ポリシー
    - オブジェクトの削除
  - **トラスト・プロビジョニング**
  - **マルチテナント・システム**
    - 認証鍵の作成
    - マルチ・レベルSCP
  - **セキュリティの推奨事項**
  - **機能の推奨事項**

注： SE050F FIPS認定済みモジュールのUGMについては、Docstore（7337xx）で提供されているAN13482を参照してください。

2 SE050Eの基礎

この章では、ユーザーがSE050Eを使用開始できるように、SE050Eについての基礎を説明します。APDU仕様に記載されている定義とコンセプトを簡単に解説します（[1]を参照）。

2.1 製品情報

SE050Eの製品IDは、セキュア・エレメントに専用のコマンドを送信することで取得できます。

Plug & Trustミドルウェア（nxp.jp）には、接続したSE050E製品から詳細な製品情報を取得するための、「se05x_GetInfo」というユーティリティが含まれています。これはWindowsバイナリ(binaries¥ex¥VCOM-se05x_GetInfo.exe) として、またはソース・コードで使用できます。Plug & Trustミドルウェア・パッケージに付属するHTMLドキュメント（「Demo & Examples」>「SE05X Get Info example」セクション）には、このユーティリティの使用とコンパイルに関するその他の情報が記載されています。Plug & Trustミドルウェアの実行に必要な追加のハードウェアを設定するには、いずれかのEdgeLock™ SE05xクイック・スタート・ガイド（ [13]など）の手順に従ってください。

se05x_GetInfoによって取得される情報は、エラッタ・シート内の項目が製品に適用可能かどうかを判別するために必要な情報の上位集合です。

正しい製品IDは以下の2つのパラメータで構成されます。

- JXXXXXXXXXXXXXXXX形式の製品OS構成（プラットフォーム・ビルドID）。
  以下の例： J3R351029B411100
- xx.xx.xx（メジャー.マイナー.パッチ）形式のアプレット・バージョン。
  以下の例：7.2.0

SE050Eの使用可能な機能と構成については、[2]を参照してください。

```
App   :INFO :PlugAndTrust_v04.00.01_20211214.0019.2
sss   :INFO :atr (Len=35)
      01 A0 00 00    03 96 04 03    E8 00 FE 02    0B 03 E8 00
      01 00 00 00    00 64 13 88    0A 00 65 53    45 30 35 31
      00 00 00

sss   :INFO :atr (Len=35)
      01 A0 00 00    03 96 04 03    E8 00 FE 02    0B 03 E8 00
      01 00 00 00    00 64 13 88    0A 00 65 53    45 30 35 31
      00 00 00
App
  :WARN :#####################################################
App   :INFO :uid (Len=18)
      04 00 50 01    CF 16 B2 06    12 D2 38 04    2C 02 21 B0
      00 00
App
  :WARN :#####################################################
App   :INFO :Applet Major = 7
App   :INFO :Applet Minor = 2
App   :INFO :Applet patch = 0
App   :INFO :AppletConfig = 3F9F
App   :INFO :With    ECDSA_ECDH_ECDHE
App   :INFO :With    EDDSA
App   :INFO :With    DH_MONT
App   :INFO :With    HMAC
App   :INFO :WithOut RSA_PLAIN
App   :INFO :WithOut RSA_CRT
App   :INFO :With    AES
App   :INFO :With    DES
App   :INFO :With    PBKDF
App   :INFO :With    TLS
App   :INFO :With    MIFARE
App   :INFO :With    I2CM
App   :INFO :Internal = FFFF
App
  :WARN :#####################################################
App   :INFO :Tag value - proprietary data 0xFE = 0xFE
App   :INFO :Length of following data 0x45 = 0x45
App   :INFO :Tag card identification data (Len=2)
      DF 28
App   :INFO :Length of card identification data = 0x42
App   :INFO :Tag configuration ID (Must be 0x01) = 0x01
App   :INFO :Configuration ID (Len=12)
      00 01 A9 21    89 0A 6F 56    4A 23 9C 41
App   :INFO :OEF ID (Len=2)
      A9 21
App   :INFO :Tag patch ID (Must be 0x02) = 0x02
App   :INFO :Patch ID (Len=8)
      00 00 00 00    00 00 00 01
App   :INFO :Tag platform build ID1 (Must be 0x03) = 0x03
```

```
App   :INFO :Platform build ID (Len=24)
      4A 33 52 33    35 31 30 32    39 42 34 31    31 31 30 30
      1A 08 FA 50    67 B5 F2 56
App   :INFO :JCOP Platform ID = J3R351029B411100
App   :INFO :Tag FIPS mode (Must be 0x05) = 0x05
App   :INFO :FIPS mode var = 0x00
App   :INFO :Tag pre-perso state (Must be 0x07) = 0x07
App   :INFO :Bit mask of pre-perso state var = 0x00
App   :INFO :Tag ROM ID (Must be 0x08) = 0x08
App   :INFO :ROM ID (Len=8)
      2E 5A D8 84    09 C9 BA DB
App   :INFO :Status Word (SW) (Len=2)
      90 00
App   :INFO :se05x_GetInfoPlainApplet Example Success !!!...
App
  :WARN :#####################################################
App   :INFO :cplc_data.IC_fabricator (Len=2)
      47 90
App   :INFO :cplc_data.IC_type1 (Len=2)
      D3 21
App   :INFO :cplc_data.Operating_system_identifier (Len=2)
      47 00
App   :INFO :cplc_data.Operating_system_release_date (Len=2)
      00 00
App   :INFO :cplc_data.Operating_system_release_level (Len=2)
      00 00
App   :INFO :cplc_data.IC_fabrication_date (Len=2)
      13 26
App   :INFO :cplc_data.IC_Serial_number (Len=4)
      00 00 08 95
App   :INFO :cplc_data.IC_Batch_identifier (Len=2)
      58 63
App   :INFO :cplc_data.IC_module_fabricator (Len=2)
      00 00
App   :INFO :cplc_data.IC_module_packaging_date (Len=2)
      00 00
App   :INFO :cplc_data.ICC_manufacturer (Len=2)
      00 00
App   :INFO :cplc_data.IC_embedding_date (Len=2)
      00 00
App   :INFO :cplc_data.IC_OS_initializer (Len=2)
      01 2C
App   :INFO :cplc_data.IC_OS_initialization_date (Len=2)
      02 30
App   :INFO :cplc_data.IC_OS_initialization_equipment (Len=4)
      30 30 30 38
App   :INFO :cplc_data.IC_personalizer (Len=2)
      00 00
App   :INFO :cplc_data.IC_personalization_date (Len=2)
      00 00
App   :INFO :cplc_data.IC_personalization_equipment_ID (Len=4)
      00 00 00 00
App   :INFO :cplc_data.SW (Len=2)
      90 00
App   :INFO :ex_sss Finished
```

2.2 未認証ユーザー

シングルテナントのユース・ケースでは、以下の両方の条件を満たした場合にユーザーがSE050Eの機能を認証なしで使用できます。

- （複数の）ユーザー間でやり取りが発生しない
- 他のユーザーから認証情報を保護するためのアクセス制御が必要ない

2.3 プラットフォームSCP

提供されるSE050Eデバイスには、OEFに基づくデバイス・タイプごとに同じ鍵を含むSCP03ベース鍵セットがデフォルトで付属します（ダイ固有ではなく、[2]で指定されているデバイス・タイプごとの鍵）。プラットフォームSCPで使用される暗号鍵の使用目的と詳細については、[10]を参照してください。

ホスト・プロセッサとセキュア・エレメント間の通信を保護したいユーザーは、SCP03をプラットフォーム・レベルで使用できます。ベース鍵を更新するための鍵管理を含むこのセキュア・チャネルは、GlobalPlatformコマンドで完全に管理でき、SE050E固有のコマンドは必要ありません。

2.4 無制限ユーザー

プラットフォーム・レベルでの認証とは無関係に、ユーザーにアプレットへの認証は適用されません。これを**無制限**ユーザーと呼びます。制限ユーザーの詳細は、「セッション」 セクションで説明します。

2.5 セキュア・オブジェクト

SE050E内に保存されているものやSE050E内で生成されたものは、すべてセキュア・オブジェクトです。

2.5.1 セキュア・オブジェクト・タイプ

サポート対象のセキュア・オブジェクト・タイプは、以下のとおりです。

- **鍵**
  - ECKey = サポート対象の楕円曲線上の非対称鍵
  - RSAKey = 512、1024、1152、2048、3078、または4096ビットのRSA（rawまたはCRT形式）用の非対称鍵
  - AESKey = 128、192、または256ビットの対称鍵。AES暗号化処理に使用されます
  - DESKey = 8、16、または24バイトの対称鍵。DES処理に使用されます
  - HMACKey = 1バイト～最長256バイトの対称鍵。HMACおよびHKDF処理に使用されます
- **ファイル**
  - BinaryFile = バイト配列（汎用ストレージ）
  - Counter = モノトニック・カウンタ
  - PCR = 追加データによって拡張できるハッシュ値
  - UserID = セキュア・オブジェクトをグループ化して関連セッションで使用可能にするために使用できる4～16バイト長のユーザー識別文字列（ホストMCU/MPU上の信頼できるオペレーティング・システムがアプリケーションIDなどに基づきアプリケーションを分離しているようなユース・ケース向け）。

詳細については、 [1] を参照してください。

2.5.2 セキュア・オブジェクト属性

セキュア・オブジェクト属性は、いずれかのセキュア・オブジェクトにリンクされます。
各属性は以下のとおりです。

- オブジェクトID = セキュア・オブジェクトの一意のID
- タイプ = セキュア・オブジェクト・タイプ
- ポリシー = セキュア・オブジェクトに適用できるアクセス制御
- 取得元 = 外部データ、内部データ、またはプロビジョニングしたデータの取得元
- 追加属性（マルチテナントにのみ適用。セクション5を参照）
  - 認証属性
  - オブジェクト・カウンタ
  - 認証オブジェクトID
  - 最大認証試行回数
  - 最小出力長
  - AEAD処理の最小タグ長

2.5.2.1 オブジェクトID

オブジェクトIDは、オブジェクトのライフタイム中には変更できないため、オブジェクトが削除されるまで同じ状態を維持します。

オブジェクトIDは常に外部で定義され、SE050Eがオブジェクトに（自動的に）割り当てることはありません。ただし、特定のユース・ケースに使用するために割り当てられる一連の予約済みIDがあります。詳細については、[1]および[2]を参照してください。

NXPがEase Of Use設定の一部として事前にトラスト・プロビジョニングしたすべての認証情報に、表1の「アプレット予約済みエリア」または「NXP予約済み領域」の範囲内のIDが含まれています。独自のセキュア・オブジェクトを作成するお客様には、「フィールド内使用」の範囲内のIDを使用することをお勧めします。

表1.アプレット予約済みエリアまたはNXP予約済み領域のID

アドレス範囲	ID
0x00000000-0x7BFFFFFF	フィールド内使用
0x7C000000-0x7CFFFFFF	Android Key Masterエリア
0x7D000000-0x7DFFFFFF	デモ・エリア
0x7FFF0000-0x7FFFFFFF	アプレット予約済みエリア
0x80000000-0xFFFFFFFF	NXP予約済みエリア

2.5.2.2 タイプ

「セキュア・オブジェクト・タイプ」を参照してください。

2.5.2.3 ポリシー

セキュア・オブジェクト・ポリシーでは、各ユーザーが実行できる操作を指定することにより、セキュア・オブジェクトへのアクセス制御を定義します。

アクセス制御を行うには、ユーザーがシステムのユース・ケースに従ってポリシーを設定しなければなりません（「セキュア・オブジェクト・ポリシー」セクションを参照）。どのセキュア・オブジェクトにも、各ユーザーの最小アクセス制御ポリシーを設定する必要があります。

セキュア・オブジェクトの作成時に明示的なポリシーがオブジェクトに渡されていない場合は、[1]で指定されているデフォルト・ポリシーが、[2]で説明されているSE050E製品で使用可能な機能に基づき適用されます。

セキュア・オブジェクト・ポリシーはオブジェクト作成時に割り当てられ、その後は変更できないため、セキュア・オブジェクトのライフタイム全体にわたって同じ状態が保たれます。

2.5.2.4 取得元

取得元属性は、セキュア・オブジェクトのコンテンツの取得元として、外部で生成されたか、内部で生成されたか、NXPによってトラスト・プロビジョニングされたかを示します。

3 SE050E Plug &Trust：標準設定で使用

3.1 Ease of Use設定

すべての汎用SE050E製品で、プロファイルに従った事前プロビジョニングが提供されます。現在利用可能な製品はE、Fです。

詳細については、[2]を参照してください。

注： SE050F FIPS認定済みモジュールのUGMについては、Docstore（7337xx）で提供されているAN13482を参照してください。

3.2 シングルテナントの保護

コンフィギュレータには、SE050Eをエンド・ユーザーのアプリケーションで使用できる状態にする責任があります。

コンフィギュレータとエンド・ユーザーは、プロトタイピングを目的とした開発者など、同じエンティティである場合もあります。

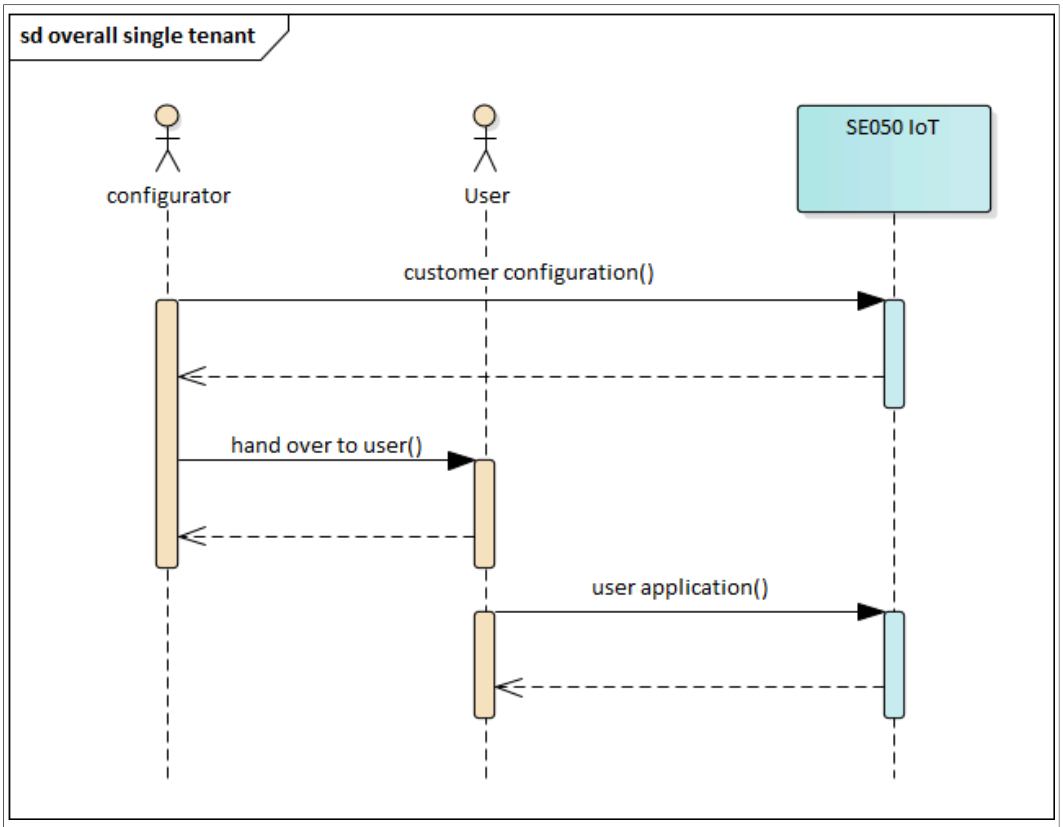

図2.シングルテナントでの使用の概要

注：

コンフィギュレータとユーザーは同じエンティティの場合もある

3.3 プラットフォームSCPの鍵を更新する方法

プラットフォームのデフォルト鍵は[2]から入手できます。

SCP03ベース鍵は、[10]で説明されているように、設定する新しい鍵の暗号鍵として既存のDEK鍵を使用することで更新できます。

Plug & Trustミドルウェアには、プラットフォームSCP03の鍵をローテートする（更新する）プログラム例が含まれています。

プログラム例とその他のドキュメントは、デモ・フォルダ内にあります。

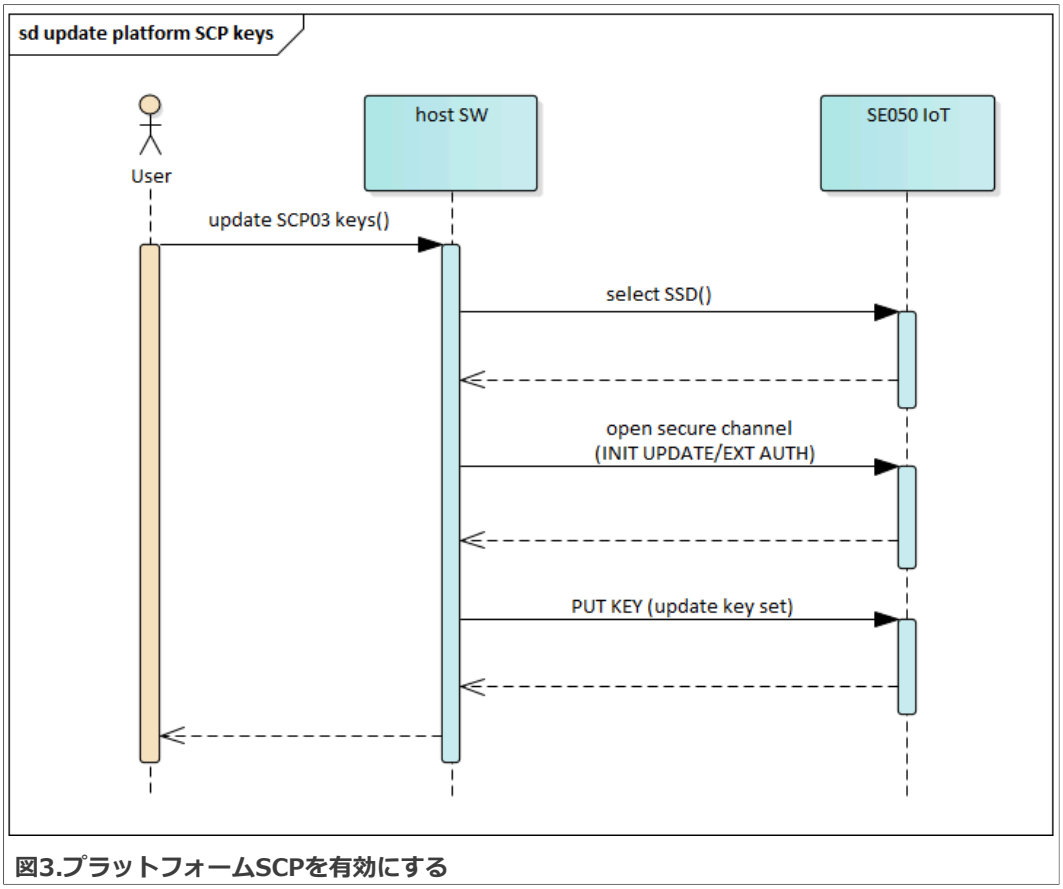

図3.プラットフォームSCPを有効にする

3.4 証明

証明は、データがセキュア・エレメント内にあることを明確に示す手段であり、I²Cコントローラの応答を証明する場合は、データが接続されたI²Cバスからのものであることを証明します。セキュア・エレメントは、NXPによってトラスト・プロビジョニングされた証明鍵で署名することにより、データの取得元を「証明」します。ユーザーから鍵またはファイル・データが要求されるとき、そのユーザーは返されるデータの証明を要求できます。証明は、要求されるデータの応答にチップ固有のID + フレッシュネス（ランダム値） + タイムスタンプ（モノトニック・カウンタ値） + ペイロード全体（要求されるデータ + 固有のID + フレッシュネス + タイムスタンプ）に対する署名を追加することで実現します。

すべての汎用SE050製品に、NXPによってトラスト・プロビジョニングされた証明鍵が付属します。一部のSE050製品には、証明鍵に関連付けられているNXPが署名した証明書も含まれています。SE050Eの設定プロファイルの詳細については、[2]を参照してください。

証明書への署名はNXPの信頼の基点エンティティによって行われます。証明には、発行済みの証明書によって保証されている信頼が必要です。証明の正当性を検証するため、証明対象のオブジェクトの署名が証明用の証明書と照合されます。

証明におけるセキュリティの推奨事項については、「証明」で詳しく説明します。

ユース・ケース

1. 生成された鍵の証明
   SE050Eは鍵を内部で生成できます。鍵がSE050E内部で生成されたことを証明するために、この証明メカニズムが使用されます。
2. 外部データの証明

お客様はSE050E内部にデータの導入やプロビジョニングを行えます。この証明メカニズムを使用することで、データが変更されずにセキュア・エレメント内に保存されていることを証明できます。

詳細については、「プロビジョニングされたオブジェクトの証明」を参照してください。

4 SE050E設定の拡張性

この章では、SE050E製品やカスタムEdgeLock製品を、Ease of Use設定に加えカスタマイズした鍵と認証情報で拡張したいと考えているユーザーおよびお客様に情報を提供します。

SE050E Ease of Use設定を拡張するためのセキュリティの推奨事項については、「拡張性とマルチテナント」を参照してください。

4.1 セキュア・オブジェクトの追加

ユーザーは新しいセキュア・オブジェクトを作成することで、Ease of Use設定にセキュア・オブジェクトを追加できます。作成時にユーザーはオブジェクトIDを割り当てる必要があります（「オブジェクトID」を参照）。アクセス制御を行うには、ユーザーがシステムのユース・ケースに従ってポリシーを設定しなければなりません（「セキュア・オブジェクト・ポリシー」セクションを参照）。どのセキュア・オブジェクトにも、各ユーザーの最小アクセス制御ポリシーを設定する必要があります。

ユーザーは永続的セキュア・オブジェクトと一時的セキュア・オブジェクトのいずれかを選択する必要があります（両方がサポートされている場合。[1]を参照）。永続的セキュア・オブジェクトの値は常にNVMに書き込まれる一方、一時的セキュア・オブジェクトの値はRAMに書き込まれます。

一時的セキュア・オブジェクトの場合は、セキュア・オブジェクトの値を（暗号化した形式で）ホスト・コントローラにエクスポートでき、SE050Eからセキュア・オブジェクトが削除されない限り、後でその値を再度インポートできます。永続的セキュア・オブジェクトは、エクスポートもインポートもできません。セキュア・オブジェクトをインポートおよびエクスポートするには、POLICY_OBJ_ALLOW_IMPORT_EXPORTポリシーを設定する必要があります。未認証のユーザー・グループによる再インポートを防ぐには、POLICY_OBJ_ALLOW_IMPORT_EXPORTを適切な認証情報に制限しなければなりません。セキュア・オブジェクト属性が変更されるのを防ぐには、POLICY_OBJ_ALLOW_DELETEポリシーを適切な認証情報にバインドして、削除を制限しなければなりません。

4.2 予約済みID

サービス妨害攻撃を防ぐには、NXPによって事前プロビジョニングされていない、セキュア・オブジェクトの予約済みIDを作成しなければなりません（できればデバイス固有の値にします）。

この点は、特に以下のIDで重要です。

- RESERVED_ID_TRANSPORT
- RESERVED_ID_FACTORY_RESET
- RESERVED_ID_I2CM_ACCESS
- RESERVED_ID_RESTRICT

4.3 暗号オブジェクトの作成

デフォルトでは、ユーザーが暗号化、署名、またはダイジェスト処理を一度に実行できるため、入力データがSE050Eに渡されると、出力データが直接返されることになります。そのような場合、SE050Eの状態は維持されません。

ただし、ユーザーがその暗号化、署名、またはダイジェスト処理のいずれかで、複数のブロックを連続してSE050Eに渡す必要がある場合は、暗号オブジェクトを割り当てることができます。

暗号オブジェクトは暗号化処理の状態を保持し、通常は初期化/（n回の）更新/終了処理を行えます。

4.4 証明鍵の追加

お客様は独自の証明鍵（および関連する証明書）を指定することで、「証明」で説明されているように証明を実行できます。これらの鍵は、セキュアな環境内で、またはセキュアなチャネルを介して導入したり生成したりしなければなりません。

4.5 クラウド接続鍵の追加

SE050E Ease of Use設定を認証情報で拡張することにより、各種クラウドへのセキュアなオンボーディングと接続を行えます。お客様が独自のPKIとCAを使用することも可能です。

このユース・ケースの詳細については、[3] および [4]を参照してください。

4.6 トランスポート・ロックの適用

「トランスポート・ロックの使用」では、トランスポート・ロックを安全に使用するためのセキュリティの推奨事項について説明します。

4.6.1 シンプルなユース・ケース

トランスポート・ロックは、物流上のモジュールを保護するために使用できるセキュア・オブジェクトです。

トランスポート・ロックはエンティティAとエンティティB間のタンパ・シールとして使用できます。エンティティAがロックを適用して鍵をエンティティBと共有することにより、エンティティBにのみアクセス権限を与えます。この場合は、エンティティBがデバイスの最終的な受領者になることができます。

4.6.2 更新可能なトランスポート・ロック

物流上に3つ以上のエンティティが存在する場合もあります。このシナリオでは、各エンティティがお客様にもコンフィギュレータにもなることができます。

カスケード型の物流の場合は、エンティティAがトランスポート・ロックを更新可能にできます。

製品を受け取ったエンティティBがAのロックを解除し、物流上の先のエンティティのためにロックを更新することができます。

エンティティBは製品を受け取るエンティティごとに特定のロックを適用することもできます。

4.7 ファクトリ・リセット

鍵のファクトリ・リセットを利用すれば、取得元属性が「プロビジョニング」に設定されているものを除き、すべてのオブジェクトを削除できます。これが該当するのは、NXP Ease of Use設定に属しているすべての鍵とUUIDなどの必須セキュア・オブジェクトです。

鍵が意図せず削除されるのを防ぐには、RESERVED_ID_FACTORY_RESETというIDのセキュア・オブジェクトを設定しなければなりません。

注： NXPによってトラスト・プロビジョニングされた証明書は、ファクトリ・リセット後に削除されます。

注： プラットフォームSCPの鍵は、ファクトリ・リセット手順による影響を受けません。

4.8 オブジェクトの削除

前述したように、クラウド・オンボーディング証明書など、Ease of Use設定に導入された認証情報の一部は、必要に応じてお客様が削除できます。

削除するには、まずその認証情報を上書きしなければなりません。そうすることで取得元が「プロビジョニング」から（書き込み方法に応じて）「内部」または「外部」に変化し、個別削除またはファクトリ・リセットによって削除できるようになります。

注： deleteAllコマンドが正しく実行されるようにするには、ReadIDListコマンドまたは個別のCheckObjectExistsコマンドを（R-MACを使用した）セキュア・チャネルの保護の下で実行し、以前からあるオブジェクトが適切に削除されるようにしなければなりません。オブジェクトが正しく削除されたことが応答に示されている必要があります。

4.9 外部オブジェクトのインポート

注： APDU「ImportExternalObject」は、まずNXPに問い合わせて潜在的な問題を回避してからでなければ、使用してはいけません。APDU「ImportExternalObject」を使用した場合、または使用する予定がある場合は、必ずNXPの担当者にご連絡ください。

ユーザーはimportExternalObjectを使用するか、アプレットSCP03またはECKeyセッションを使用して新しいオブジェクトに書き込むことで、認証情報をインポートできます。

ImportExternalObjectは、DisableSecureObjectCreationやTransportLockによって無効化されていない限り、WriteSecureObjectと同様にすべてのユーザーが実行できます。SE050Eの鍵ペア（ID 0x7FFF0202、RESERVED_ID_EXTERNAL_IMPORT）は、[2]で指定されているとおり、すでにNXPによってプロビジョニングされています。この機能を使用するには、外部ユーザーの公開鍵を認証オブジェクトとして、他の選択したセキュア・オブジェクトIDに挿入する必要があります。

認証情報の書き込みや更新を行うコマンドを送信できます。保護されていないコマンドだけでなく、ImportExternalObjectコマンドにも署名、暗号化、暗黙的な認証が行われます。

ImportExternalObjectのAPDUはリプレイできます。セキュア・オブジェクトのポリシーやバージョニングを通じてアクセス制御を使用することで、これを制限できます。

なお、APDU「WriteECKey」および「WriteRSAKey」では、書き込まれるコンポーネントの一貫性はチェックされません。また、既存のオブジェクトに対して実行する場合、APDUでP1_KeyTypeのチェックは行われません。

APDU「WriteECKey」は鍵コンポーネントを切り詰め、曲線ID_ECC_MONT_DH_448のECKeyオブジェクトを曲線ID_ECC_ED_25519の既存ECKeyオブジェクトに書き込むときにエラーは返しません。

APDU「WriteSecureObject」を既存オブジェクトに対して実行した場合、「認証インジケータ」、「AEAD処理の最小タグ長」、「最小出力長」、または「最大認証試行回数」の属性チェックは行われません。APDU「WriteECKey」のポリシー・チェックは、既存ECKeyオブジェクトの曲線の検証には対応していません。

4.10 シングルテナントのユース・ケース

4.10.1 クラウド接続

Ease of Use設定を使用することにより、各種クラウドへのセキュアなオンボーディングと接続を行えます。詳細については、以下のアプリケーション・ノートを参照してください。

- SE05xによるAzure IoT Hubへのセキュアな接続

- SE05xによるAWS IoT Coreへのセキュアな接続
- SE05xによるOEM Cloudへのセキュアな接続
- SE05xによるGCPへのセキュアな接続
- SE05xによるIBM Watson IoTへのセキュアな接続

4.10.2 デバイス間認証

すべてのSE050E製品に認証情報が事前プロビジョニングされており、それをデバイス間認証に使用できます。

ユース・ケースの詳細については、[8]を参照してください。

4.10.3 プロビジョニングされたオブジェクトの証明

証明を行うには、証明（署名）を実行する鍵ペアを信頼できる証明書チェーンに含める必要があります。

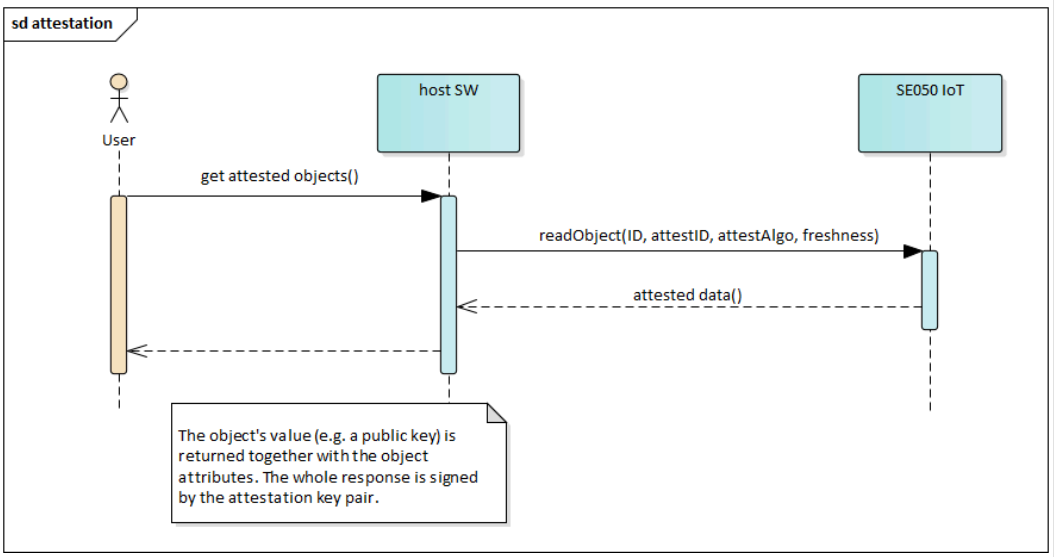

図4.証明を使用したオブジェクトの読み取り

4.10.4 ユーザー・アプリケーション

デフォルト・セッションですべてのコマンドを送信できます（アプレットへの認証もコマンドのラッピングも必要ありません）。

データはプラットフォームSCPによって暗号化されて保護されます。

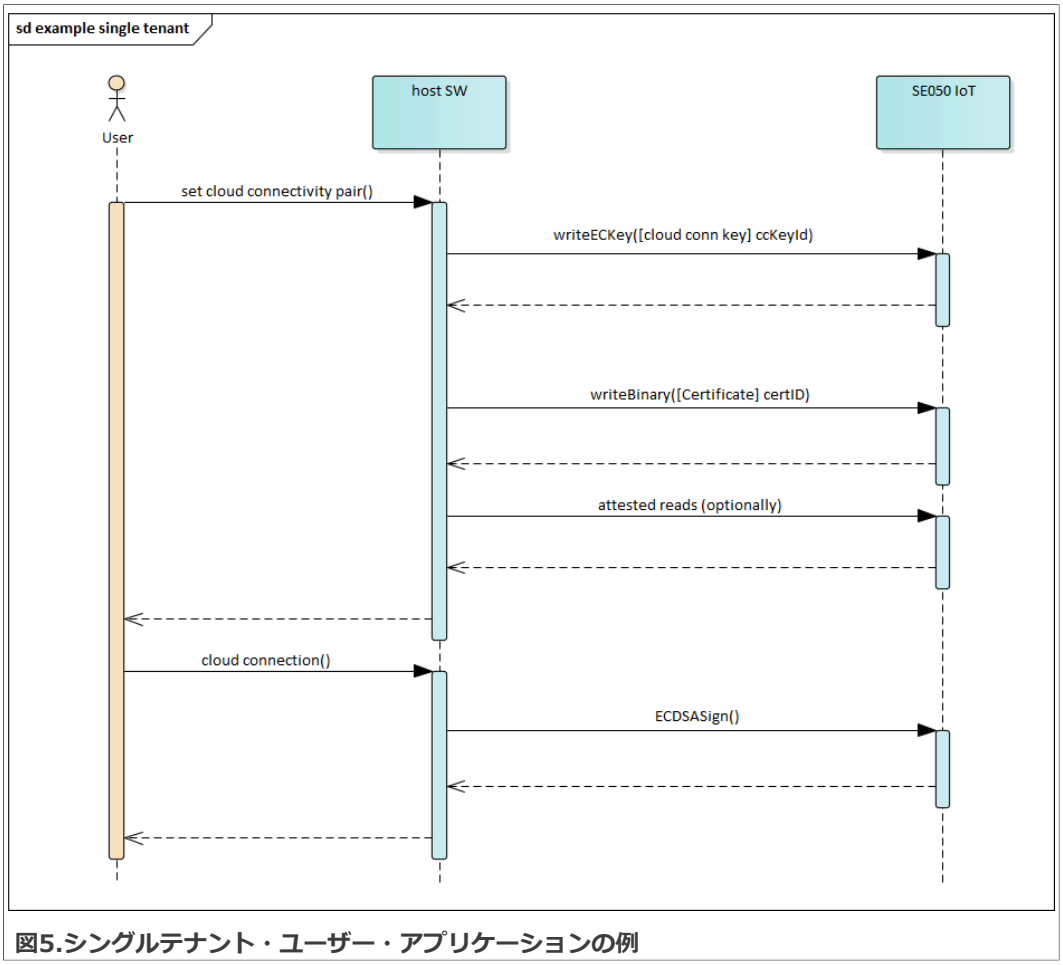

図5.シングルテナント・ユーザー・アプリケーションの例

5 マルチテナントでのSE050Eの使用

5.1 マルチテナントで使用するためのSE050Eの機能

5.1.1 認証オブジェクト

認証オブジェクトは、ユーザーがSE050Eアプレットに対して相互に認証できるようにする特別なセキュア・オブジェクトです。その点で、このオブジェクトの価値はSE050Eへのアクセスを保護することであると言えます。

認証オブジェクトを使用し、SE050Eアプレットに対して認証するユーザーは、（無制限ユーザーの対語として）**制限**ユーザーと呼ばれます。

5.1.1.1 認証オブジェクトの作成

認証オブジェクトを作成するエンティティは、**認証オブジェクト所有者** と呼ばれます。所有者は単一のエンティティの場合もあれば複数のエンティティの場合もあります（認証オブジェクトの値を知っているユーザー）。

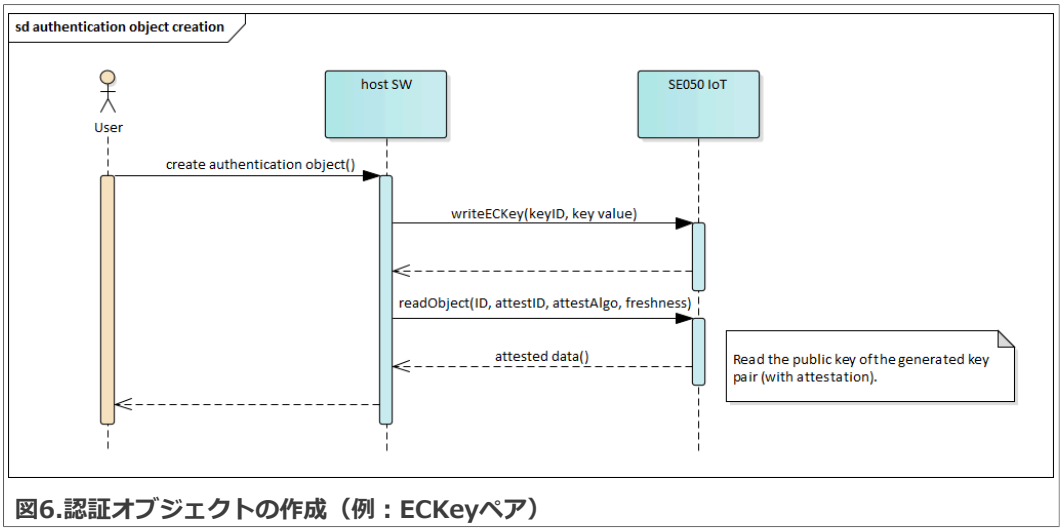

図6.認証オブジェクトの作成（例：ECKeyペア）

5.1.2 セッション

SE050Eでは、以下のいずれかのセキュア・オブジェクトで**セッション**を開くことができます。

- userID （UserIDセッションを開く）
- AES128 鍵（SCP03セッションを開く）
- ECKeyペアまたはEC公開鍵（ECKeyセッションを開く）

UserIDセッションには平文での通信が使用されますが、SCP03またはECKeyセッションにはSCP03セキュア・メッセージングが使用されるため、エンドツーエンドの保護が得られます（セキュリティの推奨事項を参照）。

ユーザーがセッションを開くと：

- 無制限ユーザーのアクセス権限は適用されなくなります。
- セッションを開くために使用された認証オブジェクトIDによってユーザーが認識され、**制限**ユーザーになります。

デフォルトでは、SCP03またはECKeyセッションが確立されると、そのセッションに**アプレット・レベルのSCP**がエンドツーエンドで適用されます。アプレット・レベルでは、SCPはSCP03セキュア・メッセージングを使用します。SCP03セッションとECKeyセッションの違いは認証方法であり、SCP03が対称暗号化をベースにしているのに対し、ECKeyは認証に非対称暗号化を使用しています。

認証済みユーザー・セッションに関するセクションでは、セッションを安全に使用するための推奨事項について説明します。

なお、プラットフォームSCPが使用されている場合は、アプレット・レベルのSCPはプラットフォームSCPチャネルの内部にラッピングされます。[1]を参照してください。

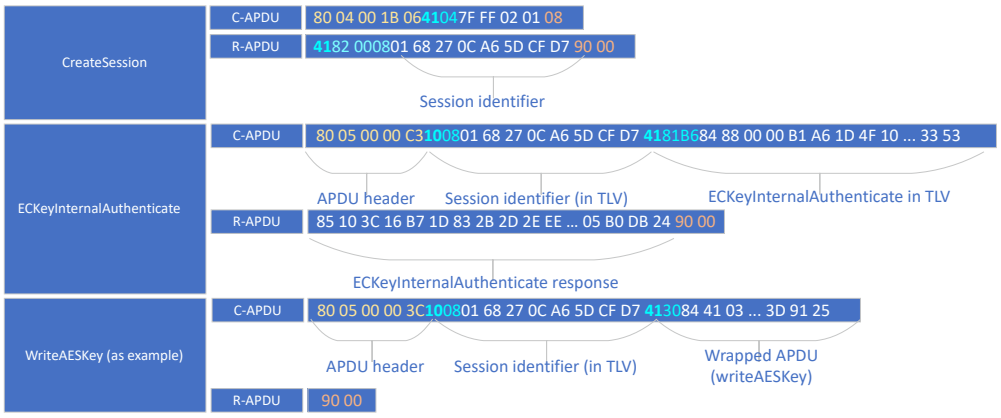

図7.プラットフォームSCPを使用しないECKeyセッションでのAPDUの例

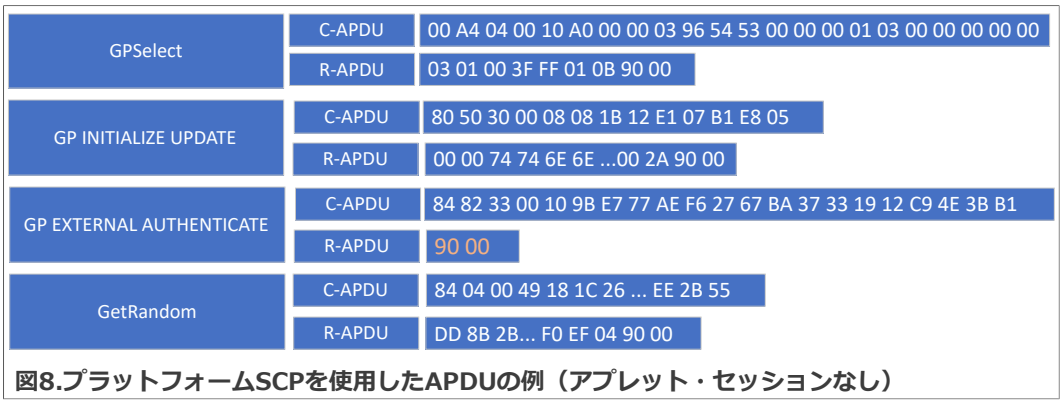

図8.プラットフォームSCPを使用したAPDUの例（アプレット・セッションなし）

5.1.2.1 セッション・ポリシー

セキュア・オブジェクト・ポリシーに加え、ユーザーはセッションにもポリシーを割り当てることができます。セッションの作成時にポリシーが引数として渡されると、セッションのライフタイムはセッション内に送信されるAPDUの数に制限されます。つまりユーザーがAPDUの最大数を渡すと、その最大数に達した時点でセッションが終了し、ユーザーは認証された状態ではなくなります。

なお、ユーザーがSessionRefreshを呼び出すことで、セッションのライフタイムを延長できます。

5.1.2.2 UserIDセッションの例

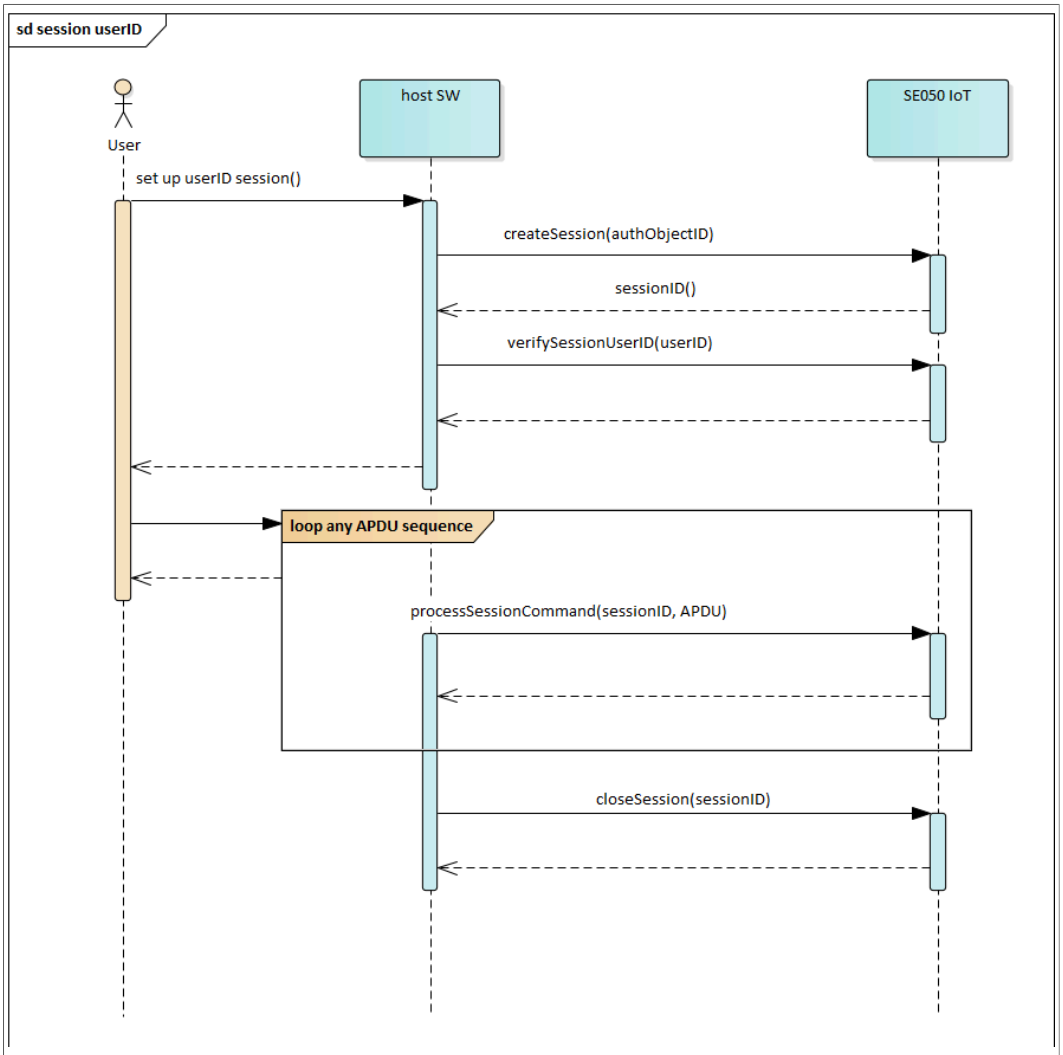

図9.UserIDセッションの例

注： デフォルト・セッション・ポリシー

5.1.2.3 SCP03セッションの例

ここでは、GlobalPlatform（Card Specification v 2.2 – 修正条項D）で定義されているSCP03プロトコルが使用されています。GlobalPlatform SCP03セッションは、以下の図に示されているようにアプレット・セッション内にカプセル化され、「アプレットSCP03セッション」と呼ばれます。

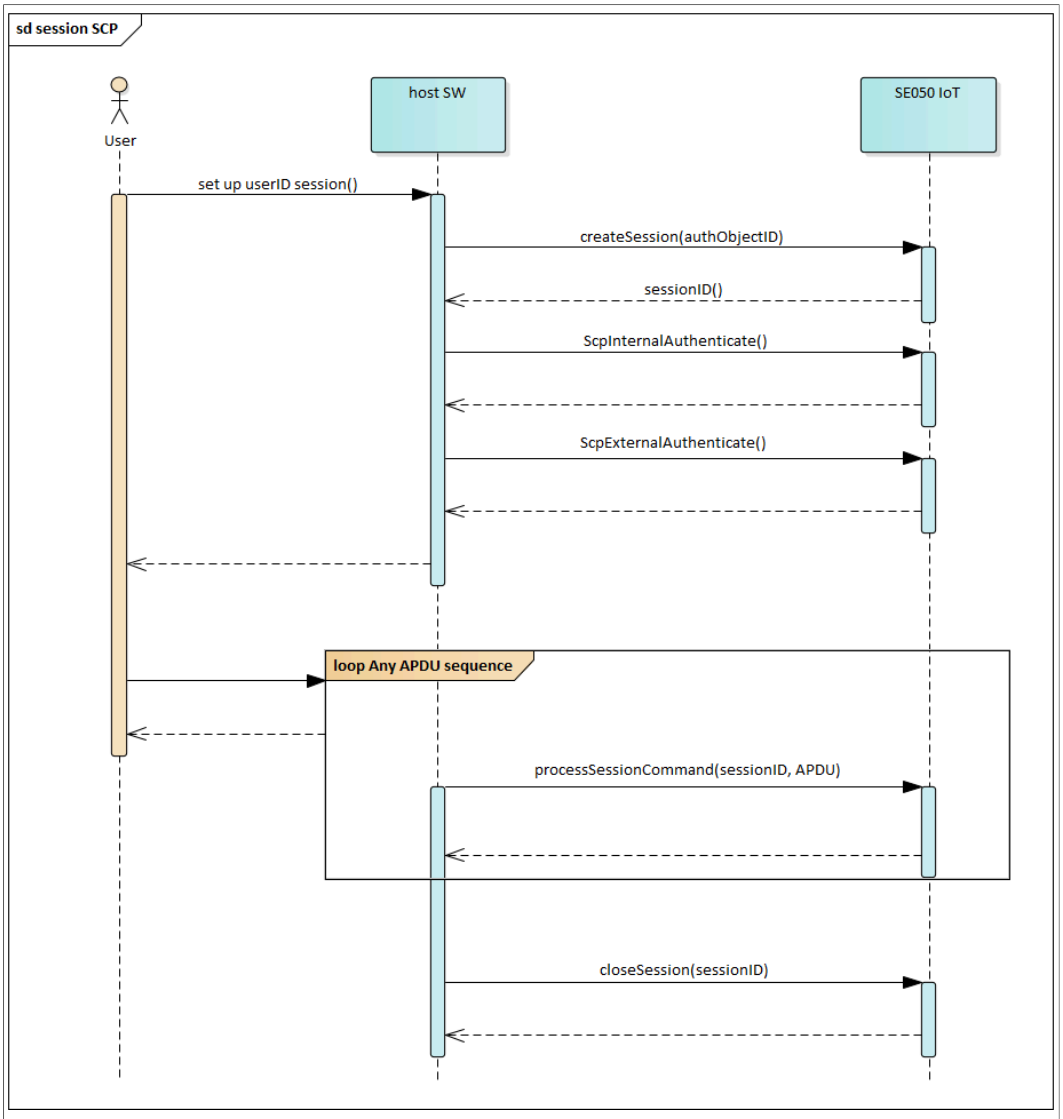

図10.SCPセッションの例

注： デフォルト・セッション・ポリシー

5.1.2.4 ECKeyセッションの例

ECKeyセッションでは、SE050Eに保存されているECKeyを使用して制限ユーザー・セッションを開きます。認証は非対称ECKeyを使用して行われ、セッションはSCP03プロトコルを使用して暗号化されます。ECKey認証は、[1]で定義されています。

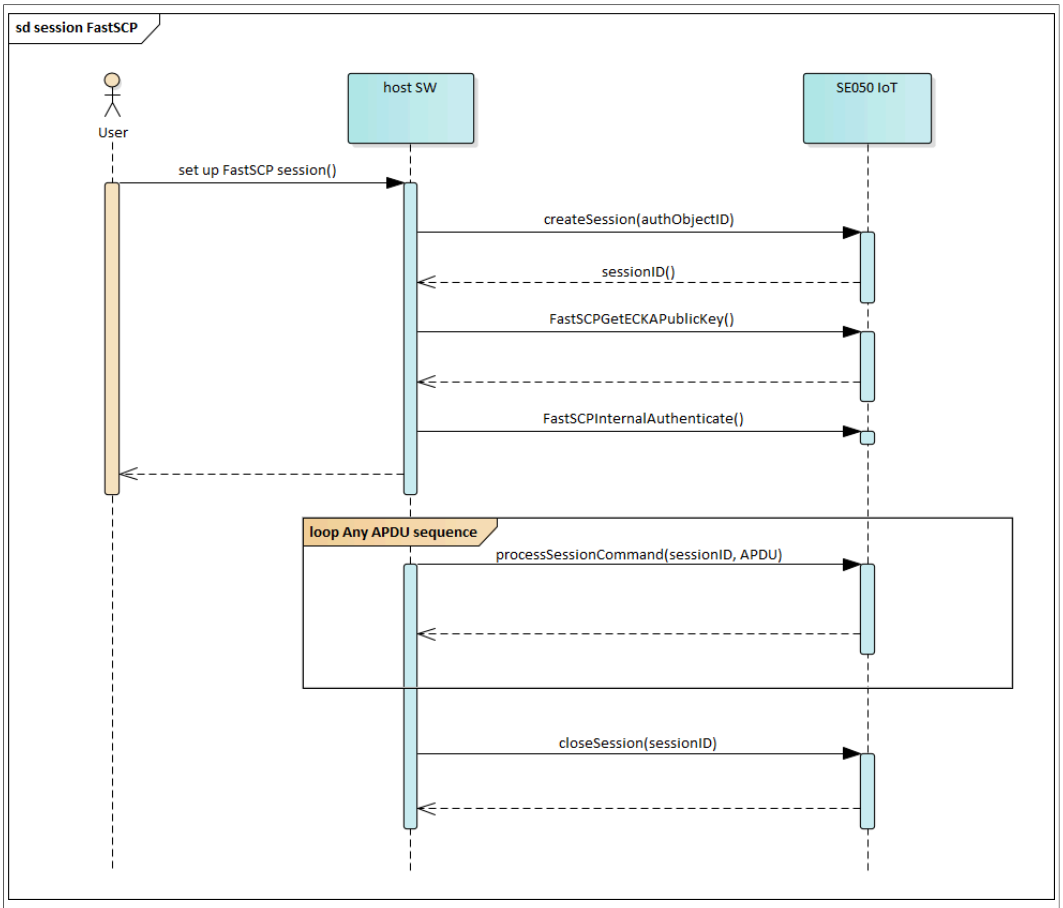

図11.ECKeyセッションの例

注： デフォルト・セッション・ポリシー

5.1.3 マルチテナントで使用するためのセキュア・オブジェクト・ポリシー

複数のユーザーが構成または想定されている場合、セキュア・オブジェクト・ポリシーを設定して、適切なユーザーが正しい操作を行えるようにする（および不適切なユーザーによる操作を禁止する）必要があります。

（シンプルな）例としては、以下のようなオブジェクト・ポリシーへのユーザーのマッピングが挙げられます。

表2.マルチテナントで使用するためのセキュア・オブジェクト・ポリシー

	ユーザーA	ユーザーB
POLICY_OBJ_ALLOW_DELETE	付与	拒否
POLICY_OBJ_ALLOW_READ	付与	付与
POLICY_OBJ_ALLOW_WRITE	付与	拒否
POLICY_OBJ_ALLOW_SIGN	拒否	付与

6 トラスト・プロビジョニング

この章では、認証情報のプロビジョニングに焦点を絞って説明します。

「認証情報のプロビジョニング」では、SE050Eで安全に認証情報をプロビジョニングする方法についての推奨事項を説明します。

6.1 信頼できる環境または信頼できない環境

デバイスのプロビジョニング段階は、機密性の高いデータや重要な素材がSE050Eで生成されたり、SE050Eに導入されたりするため、製品のセキュリティにとって非常に重要です。

デバイスは以下の異なるタイプの環境で動作できます。

- **信頼できる環境** – 信頼できる環境とは、信頼できる機関の制御下にあるセキュリティの確保された環境です。セキュリティのレベルは環境によって異なり、デバイスとその資産に関連する脅威やセキュリティ目標に適したレベルを設定する必要があります。
- **信頼できない環境** – 信頼できない環境とは、セキュリティが確保されておらず、何の制御も適用できない環境です。

6.2 SE050Eトラスト・プロビジョニング

デバイス登録の試行やOEMサーバにアップロードされるデータを信頼できるようにするため、IoTデバイスのIDは、検証可能かつ信頼できる一意のIDである必要があります。SE050Eは、OEMクラウド・サービスへのデバイスの認証および登録に必要な鍵と認証情報を安全に保存できる、改ざん耐性のあるプラットフォームを提供するよう設計されています。SE050Eセキュリティ ICを活用することで、OEMはセキュリティ・コードを記述したり認証情報や鍵をさらしたりすることなく、安全にデバイスを認証できます。

EdgeLock SE050EセキュリティICのプロビジョニングでは、以下のオプションを利用できます。

- EdgeLock 2GO Ready：すべてのEdgeLock SE050E製品に鍵が事前プロビジョニングされており、それをデバイス間認証を含むすべての主要ユース・ケースに使用できます。
- EdgeLock 2GO Custom：NXPでは、SE050E ICの製造時に必要な認証情報を導入するためのカスタマイズ・サービスを提供しています。このサービスの詳細については、NXPにお問い合わせください。
- EdgeLock 2GO Managed：NXPでは、SE050Eをリモートで設定するためのクラウド・サービスを提供しています。EdgeLock 2GO Managedは、デバイスに必要な鍵と認証情報をプロビジョニングし、デバイス認証情報のライフサイクルを管理するための、セキュアで柔軟な方法です。詳細情報と評価アカウントのリクエストについては、www.nxp.jp/EdgeLock2GOをご覧ください。
- OEM、販売代理店、サードパーティ・パートナーによってプロビジョニングされるEdgeLock SE050E：OEMはEdgeLock SE050Eを独自にプロビジョニングすることも、SE050Eのプロビジョニングを行う販売代理店やサードパーティ・パートナーを選択することもできます。

7 セキュリティの推奨事項

この章では、製品を安全に使用するために従う必要のある要件と推奨事項について説明します。これらを順守しないと、セキュリティ・ギャップが生じるおそれがあります。

RFC2119（[9]を参照）に準拠し、「しなければならない」、「する必要がある」、「してもよい/することができる」という表現が使用されています。

- **しなければならない** ：絶対的なセキュリティ要件

- **する必要がある** ：セキュリティの推奨事項を指し、特定の状況においては特定の条項を無視する正当な理由が存在し得ることを意味する
- **してもよい/することができる** ：ある条項が任意であることを意味する

7.1 一般的な推奨事項（すべてのユース・ケース）

7.1.1 プラットフォームおよびアプレット・レベルSCP

盗聴と悪意のあるコマンド・インジェクションからのローカルな保護のために、プラットフォームSCPまたはアプレット・レベルSCPを使用しなければなりません。

運用段階では、セキュア・オブジェクト・ポリシーによってプラットフォームSCPまたはアプレット・レベルSCPを要求するようセキュア・エレメントを設定しなければなりません。APDUインターフェースでの機密性と完全性を保証するため、フル・セキュリティ・レベル、つまりコマンドおよび応答MACと暗号化（APDU仕様を参照）を有効にしなければなりません。NXP PlugAndTrust MWは、デフォルトでフル・セキュリティ・レベルを使用します。

鍵のプロビジョニング時、セキュア・エレメント外、ホストおよびそのメモリ内では、ホストSCP鍵セットの機密性、完全性、真正性を必要に応じて強制しなければなりません。

- 使用可能な場合にホスト鍵のアクセス制御を強制するか、鍵の漏洩を防ぐ何らかのメカニズムを用意しなければなりません。
- 環境対策によってその他のセキュリティ特性を保持しなければなりません。

製品の初回使用時にデフォルトSCP鍵を更新しなければなりません。ホストとセキュア・エレメント間を相互にバインドできるようにダイ固有の鍵を使用することが推奨されます。

鍵のプロビジョニング時、SE050E外、ホストおよびそのメモリ内では、SCP鍵セットの機密性、完全性、真正性を必要に応じて強制しなければなりません。

- SCP鍵はホスト内で安全に保管しなければなりません。プラットフォームSCPを使用する場合は、暗号化 (ENC) 鍵とメッセージ認証符号 (MAC) 鍵のみをホストに保管し、鍵セットの更新に使用されるデータ暗号化 (DEK) 鍵はホストではなくSE050E内に保管することが推奨されます。プラットフォームSCPとともに使用される暗号鍵の使用目的と詳細については、[10]を参照してください。
- 使用可能な場合にホスト鍵のアクセス制御を強制するか、鍵の漏洩を防ぐ何らかのメカニズムを用意しなければなりません。
- 環境対策によってその他のセキュリティ特性を保持しなければなりません。

7.1.2 初期状態

SE050Eの受領時に、セキュア・オブジェクトのトラスト・プロビジョニング済みフラグを読み取ることにより、プロビジョニングされたセキュア・オブジェクトの真正性をチェックすることができます。

- トラスト・プロビジョニング済みフラグの存在により、セキュア・オブジェクトがNXPによって安全にプロビジョニングされていることが保証されます。

SE050Eのライフサイクル中は、セキュア・オブジェクト・コンテンツを証明モードで読み取ることにより、プロビジョニングされたセキュア・オブジェクトの真正性をチェックすることができます。

7.1.3 証明

7.1.3.1 証明鍵

証明に使用されるセキュア・オブジェクトには、POLICY_OBJ_ALLOW_ATTESTATIONを明示的に設定しなければならず、POLICY_OBJ_ALLOW_SIGNまたはPOLICY_OBJ_ALLOW_DECRYPTポリシー・ルールは、いずれも設定してはなりません。

証明鍵を使用する際は、（公開鍵に関連付けられた証明書チェーンの検証などによって）証明鍵が信頼できる状態でなければなりません。

証明に事前プロビジョニングされたセキュア・オブジェクトを使用し、既存の証明書で鍵の完全性をチェックすることが推奨されます。これが該当するのは、NXPによってトラスト・プロビジョニングされた（ORIGIN_PROVISIONEDで示されている）認証情報、および関連する証明書です。

注：「C」バージョンの製品には、事前プロビジョニングされた証明鍵用の証明書が付属します。

7.1.3.2 証明を使用した読み取り

証明を使用して読み取りを行う際は、証明の再利用を防ぐために、証明ごとに返されるすべてのフィールドをチェックしなければなりません。

- 証明の署名は信頼できる証明鍵で検証しなければなりません。
- 連続する証明のタイムスタンプ・フィールドが連続していることをチェックしなければなりません。注：タイムスタンプには前の証明付き読み取り時の値よりも小さい値が含まれていてはなりません。
- C-APDUのフレッシュネス（ユーザーが入力）は一意/ランダムでなければなりません。
- オブジェクトID、タイプ、オブジェクト属性を想定される値と照合しなければなりません。

RSAKeyまたはECKeyオブジェクトに対して証明付き読み取りを行っても、秘密鍵の正当性を示す証拠は得られません。ECKeyオブジェクトに対して証明付き読み取りを行っても、鍵の曲線の正当性を示す証拠は得られません。

7.1.4 セキュア・オブジェクト・ポリシー

セキュア・オブジェクトへのアクセス制御が必要な場合は、ユーザーがオブジェクトのポリシーを設定しなければなりません。

- NXPが定義したデフォルト・ポリシーに、エンド・ユース・ケースのアプリケーションは考慮されていません。そのようなポリシーをアプリケーションで使用できるか評価する責任は、すべて開発者が負います。NXPでは、エンド・アプリケーションのニーズとセキュリティに従ってポリシーを設定することを推奨します。
- NXPではプロトタイピングを目的としてデフォルト・ポリシーを定義しており、結果として特定のユース・ケースに必要になるよりも多くのアクセス権限を認証情報に許可することになるため、デフォルト・ポリシーの使用は推奨されません。
- アクセス制御を行うには、ユーザーがシステムのユース・ケースに従ってポリシーを設定しなければなりません（「セキュア・オブジェクト・ポリシー」セクションを参照）。どのセキュア・オブジェクトにも、各ユーザーの最小アクセス制御ポリシーを設定する必要があります。

7.1.5 鍵の使用

1つの特定の目的（署名の作成、暗号化、復号化など）のみに鍵を使用し、以下のようなユース・ケースと兼用しないようにすることが推奨されます。

- データの署名

- 証明書への署名
- 鍵の暗号化
- データの暗号化
- 鍵の共有

例：メッセージの復号化に使用される鍵を、署名の生成に使用してはいけません。これは、鍵に使用可能な低レベル暗号化処理（場合によっては同じ処理）とは無関係です。

例：データの暗号化に使用されるAES鍵を、CMACを使用したデータの署名に使用してはいけません。

7.1.6 鍵の導出関数

PBKDF2の反復カウントは、ユース・ケースごとに適切に選択しなければなりません。少ないカウントでの実行がユース・ケースのセキュリティに影響する可能性がある場合、関連するHMACKeyへのアクセスを、以下のうち少なくとも1つの方法で保護しなければなりません。

- POLICY_OBJ_REQUIRE_SMの設定
- 処理用の認証オブジェクトの設定
- プラットフォームSCPの要求

出力をR-APDUで返す代わりにターゲット・オブジェクトに格納することが関数により可能な場合は、POLICY_OBJ_FORBID_DERIVED_OUTPUTをソース・オブジェクトに適用することで、出力が外部のユーザーに返されるのを防ぎ、結果としてSE050E上のターゲット・オブジェクトの使用を要求することができます。詳細については、[1]を参照してください。

全体の処理中に操作が行われたり、さまざまな中間コマンドが実行されたりするのを防ぐため、鍵の共有と鍵の導出関数を組み合わせて連続で実行しながら（ECDHGenerateSharedSecretに続けてHKDFExtractAndExpandなど）、その中間結果をSE050Eに残すような場合は、それをセッション内で実行しなければなりません。

RSA_PSKまたはECDHE_PSK鍵交換アルゴリズムによってTLSCalculatePreMasterSecretで使用されるターゲット・オブジェクトは、2つのソース・オブジェクトのうち1つのみに対して検証されるALLOW_DERIVED_INPUTを設定しても、操作から保護することはできません。そのようなターゲット・オブジェクトを操作から保護するには、代わりにPOLICY_OBJ_REQUIRE_SMを使用し、ALLOW_DERIVED_INPUTを認証オブジェクトに制限するか、プラットフォームSCPを要求します。

HKDF resp. PDKDF2関数によって導出されたシークレットがターゲット・オブジェクトに返される場合、関連するソース・オブジェクトにその属性内の最小出力長を割り当てることにより、導出したシークレットの機密性を維持できます。

ECDHまたはECDHE_PSK鍵交換アルゴリズム用にTLSCalculatePreMasterSecretでソース・オブジェクトとして使用されるECKeyPairにPOLICY_OBJ_FORBID_DERIVED_OUTPUTを割り当てることにより、応答内の関連する共有シークレットを取得するためにECDHGenerateSharedSecretでそのECKeyPairが悪用されるのを防げます（ALLOW_KAがAPDU ECDHGenerateSharedSecretと共有されるため）。

7.1.7 暗号化処理の相互利用

7.1.7.1 暗号化処理ポリシー

AES暗号化処理のすべてのモードで暗号化に同じ暗号プリミティブが使用されており、CTR、CCM、GCM/GMACの各モードで暗号化と復号化は数学的に等価です。そのためPOLICY_OBJ_ALLOW_ENCが設定されている状態でPOLICY_OBJ_ALLOW_DECポリシーを除外しても、CTR、CCM、またはGCM/GMACモードで復号化処理を回避することはできません。

FORBID_EXTERNAL_IVをPOLICY_OBJ_ALLOW_ENCと併用することにより、IVをSE050Eで生成して返すことができます。そのためIVほど実用的ではないAES CTR、CCM、またはGCM/GMACモードでの復号化は選択できなくなります。

ECB、CBC、CTR、CCM、およびGCM/GMACのうち、POLICY_OBJ_ALLOW_DECが設定された状態でPOLICY_OBJ_ALLOW_ENCポリシーを除外することにより、暗号化処理を回避できるモードはありません。

7.1.7.2 AEADモードでの暗号化処理

関連付けられたAES CCMおよびAES GCM/GMACデータ・モードで認証した暗号化の内部認証鍵は、同じ暗号鍵を以下のモードで使用することで返されるように構築できます。

- AES CTR (ENC/DEC)
- AES ECB (ENC)
- AES CBC (ENC)

従ってPOLICY_OBJ_ALLOW_ENCが設定されている場合にAES CCMおよびAES GCM/GMACで内部認証鍵の機密性を保護するには、FORBID_EXTERNAL_IVと組み合わせなければなりません。POLICY_OBJ_ALLOW_DECポリシーが設定されているか、POLICY_OBJ_ALLOW_ENCポリシーがFORBID_EXTERNAL_IVなしで設定されている場合は、以下のうち少なくとも1つを設定して暗号鍵へのアクセスを制限しなければなりません。

- POLICY_OBJ_REQUIRE_SMの設定
- 処理用の認証オブジェクトの設定
- プラットフォームSCPの要求

7.1.8 トランスポート層のセキュリティ

RSA_PSKまたはECDHE_PSK鍵交換アルゴリズムによってTLSCalculatePreMasterSecretで使用されるターゲット・オブジェクトは、鍵ペアに対してのみ検証され、HMACKeyソース・オブジェクトに対しては検証されないALLOW_DERIVED_INPUTを設定しても、操作から完全に保護することはできません。そのようなターゲット・オブジェクトを操作から保護するには、代わりにPOLICY_OBJ_REQUIRE_SMを使用し、ALLOW_DERIVED_INPUTを認証オブジェクトにバインドするか、プラットフォームSCPを要求します。詳細については、[1]を参照してください。

7.1.9 MIFARE DESFire EV2のサポート機能

DFChangeKeyコマンドは、SE050Eに保存されている鍵を外部のMIFARE DESFireデバイスにプロビジョニングするために使用します。そのため関連するPOLICY_OBJ_ALLOW_DESFIRE_CHANGEKEYポリシーは、その用途の鍵だけに限定して適用しなければなりません。POLICY_OBJ_ALLOW_DESFIRE_CHANGEKEYポリシーは、DESFire認証鍵IDで拡張する必要があり、その鍵をDFChangeKeyの呼び出し時にDESFireで認証する必要があります。そのようなDESFire認証鍵では、POLICY_OBJ_ALLOW_DESFIRE_DUMP_SESSION_KEYを設定しないことが強く推奨されます。他のユース・ケースでセッション鍵のダンプが必要な場合、ホストはchangekeyの実行に

使用される認証セッションからセッション鍵が漏洩するのを防がなければなりません。検討可能な選択肢は以下のとおりです。

- DESFire鍵を2回設定する：
  - 1回は、POLICY_OBJ_ALLOW_DESFIRE_CHANGEKEY認証鍵を、POLICY_OBJ_ALLOW_DESFIRE_DUMP_SESSION_KEYなしで設定し、DFChangeKeyコマンドの実行に使用。
  - もう1回は、DESFire認証鍵として、POLICY_OBJ_ALLOW_DESFIRE_CHANGEKEYなし、POLICY_OBJ_ALLOW_DESFIRE_DUMP_SESSION_KEYありで設定し、他のDESFire機能に使用。
- セキュア・セッションなどによってSE050Eへのアクセスを保護し、セッション鍵がダンプされないようにする。
- ホスト内でダンプされたセッション鍵の機密性を保護し、認証セッション後にすぐ消去されるようにする。

その他のDESFire関連コマンドおよびポリシーに関する詳細と説明については、[1]を参照してください。

7.2 拡張性とマルチテナント

7.2.1 トランスポート・ロックの使用

7.2.1.1 トランスポート・ロック

エンティティAがロックをSE050Eに適用して鍵をエンティティBと共有することにより、エンティティBにのみアクセス権限を付与できます。この場合は、エンティティBがデバイスの最終的な受領者になることができます。

SE050Eの設定でトランスポート・ロックが想定されている場合、お客様はSE050Eの受領時点でまだロックが適用されていることを確認しなければなりません。

- ロック状態では、GetVersion、GetUniqueID、GetRandom、およびCreateSessionコマンドのみが許可されます。ReadIDListコマンドは失敗し、SW_COMMAND_NOT_ALLOWEDという応答が返されます。
- 想定外の動作が発生した場合は、トランスポート・ロックを適用したエンティティにそれを報告しなければなりません。

トランスポート・ロックが適用されている場合は、SE050Eのロックを解除することができます。ロックを解除したときの応答は、SW_NO_ERRORでなければなりません。

- 0x7FFF0200というIDの予約済み認証オブジェクトへの認証を行うことで、ロックを解除できます。それが失敗するか、想定外の動作が発生した場合は、NXPに報告しなければなりません。

7.2.1.2 トランスポート・ロックのプロビジョニング

これらの推奨事項は、デバイスのプロビジョニングを行うためにトランスポート・ロックを必要としている、お客様またはサードパーティのプログラミング事業者に適用されます。

トランスポート・ロックは、カスケード型物流でデバイスを他の関係者に配送するためのタンパ・シールとして使用することができます。

- このシナリオでは、トランスポート・ロックを輸送中の製品への操作を妨げるシールと考えることができます。

サプライ・チェーンで複数のお客様がプロビジョニングを実行しようとしている場合、それぞれのお客様がトランスポート・ロックを更新しなければなりません。

- この場合は、トランスポート・ロックに書き込みアクセス・ポリシーを設定しなければなりません。

7.2.2 UserIDセッション

UserIDセッションは、認証機能は備えていませんが、セキュア・オブジェクトの論理的なグループ化を行うために使用します。

7.2.2.1 UserIDセキュア・オブジェクト

UserIDセキュア・オブジェクトを安全に使用するには、最大認証試行回数であるTAG_MAX_ATTEMPTSをゼロ以外の値に設定しなければなりません。

- UserIDセキュア・オブジェクトのTAG_MAX_ATTEMPTSの値がゼロになっていると、認証の試行回数が無限になります。UserIDは総当たり攻撃による侵害を受ける可能性があります。
- なお、TAG_MAX_ATTEMPTSがゼロ以外の値になっていると、カウンタのプリデクリメントが原因で、UserIDを検証するたびにフラッシュ書き込みが発生することになります。

7.2.2.2 ユーザー・セッションでのセキュリティ要求

通信の機密性または完全性が必要な場合は、UserIDセッションを単独で使用してはなりません。

- UserIDセッションは盗聴される可能性があり、その後の通信は暗号化されないため、本質的に安全ではありません。
- 通信の機密性と完全性を確保するには、SCP03またはECKeyセッションを使用しなければなりません。

7.2.3 セキュア・メッセージング

セキュア・オブジェクトで機密性が必要な場合は、セキュア・オブジェクト・ポリシーに以下のいずれかが設定されていなければなりません。

- POLICY_OBJ_REQUIRE_SMルール。または
- 既存の鍵認証オブジェクト（SCP03セッションのAES128鍵またはECKeyセッションのECCKey）を参照する認証オブジェクトID。または
- プラットフォームSCPを強制するよう設定されている必要があります。
- C-ENC、C-MAC、R-ENC、R-MACを有効にするために最高のセキュリティ・レベルが設定されていなければなりません。

セキュア・チャネルのコンセプトとセキュア・チャネルの使用されるセキュリティ・レベルをユース・ケースに合わせて調整しなければなりません。可能な限り常に最高のセキュリティ・レベルを選択するのが理想的です。

7.2.4 ECKeyセッション

ECKeyでセキュア・セッションを確立するためのエフェメラル鍵を、ホストの静的認証秘密鍵と同じレベルのセキュリティで保護しなければなりません。そのためセキュア・チャネルが不要になった場合は破棄しなければなりません。さらに、以下の場合は毎回新しく作成したエフェメラル鍵を使用しなければなりません。

- ECKeySessionInternal認証でセキュア・チャネルが新しく確立されたとき
- ImportExternalObjectを使用してセキュア・オブジェクトが新しくインポートされたとき

SE050Eの認証のフレッシュネスを確保するには、セキュア・チャネル用のR-MACを有効にし、受け取ったMACを検証しなければなりません。

証明付きの読み取りを使用してSEの認証用の公開鍵を取得するか、証明書で公開鍵を検証することが推奨されます。

7.2.5 認証情報のプロビジョニング

これらの推奨事項は、プロビジョニングを行うお客様またはサードパーティのプログラミング事業者に適用されます。

注：アクセス権限が制限された認証済みセッションを確立することにより、プロビジョニングを保護/制限できます。

7.2.5.1 リモート・プロビジョニング

リモート・プロビジョニング時に秘密鍵を転送するには、アプレット・レベルSCPまたはセキュア・オブジェクト・インポートを使用しなければなりません。

- リモート・プロビジョニング時にシークレットのエンドツーエンドの機密性と完全性を確保するには、プラットフォームSCPに加え、アプレット・レベルSCP（SCP03またはECKeyセッション）またはセキュア・オブジェクト・インポートを使用することが必須です。

7.2.5.2 非対称鍵と鍵ペア

SE050Eにプロビジョニングされる鍵ペアの機密性、完全性、真正性は、プロビジョニング時やSE050Eの外部で使用する際に、必要に応じて強制されなければなりません。

- 秘密鍵をSE050E内に保持できるように、鍵ペアをオンチップで生成することができます。
- 環境対策によってその他のセキュリティ特性を保持しなければなりません。

オンチップで生成するEC鍵は、P1KeyTypeをP1_KEY_PAIRに設定することにより、常に鍵ペアとして生成しなければなりません。

SE050Eにプロビジョニングされる鍵ペアの完全性と真正性のみが必要な場合は、プロビジョニング済みの証明鍵によるセキュア・オブジェクトの証明を使用することができます。

SE050Eにプロビジョニングされる鍵ペアは、ダイ固有でなければなりません。

- デバイス固有の鍵ペアを使用することで、他のデバイスで成功した攻撃が有効利用されるのを防げます。

RSA鍵の公開指数は0x010001 (2^16+1) 以上を選択しなければなりません。

7.2.5.3 対称鍵

SE050Eにプロビジョニングされる対称シークレットの機密性、完全性、真正性は、プロビジョニング時やSE050Eの外部で使用する際にも、必要に応じて強制されなければなりません。

- SE050Eは、RFC3394に従ってラッピングされた鍵値の書き込みによる対称鍵をサポートしています。関連するラッピング解除鍵には、POLICY_OBJ_ALLOW_RFC3394_UNWRAPポリシーが設定されていなければならず、POLICY_OBJ_ALLOW_DECポリシーが設定されていてはなりません。
- 環境対策によってその他のセキュリティ特性を保持しなければなりません。

SE050Eにプロビジョニングされる対称鍵の完全性のみが必要な場合は、プロビジョニング済みの証明鍵によるセキュア・オブジェクトの証明を使用することができます。

- 「証明」に従って証明のタイムスタンプ・フィールドとフレッシュネス・フィールドをチェックしなければなりません。

ユース・ケースで可能な場合は、SE050Eにプロビジョニングされる対称シークレットをダイ固有にする必要があります。

- 対称鍵を使用することで、他のデバイスで成功した攻撃が有効利用されるのを防げます。

7.2.6 汎用ストレージ

SE050EにプロビジョニングされるGPデータの完全性と真正性は、プロビジョニング時やSE050Eの外部で使用する際に、必要に応じて強制されなければなりません

- SE050EにプロビジョニングされるGPデータの完全性は、プロビジョニング済みの証明鍵によるGPデータの証明によってサポートされます。
- 環境対策によってその他のセキュリティ特性を保持しなければなりません。

8 機能の推奨事項

8.1 摩耗の防止

NVM書き込みには、フラッシュが摩耗し、デバイスが永久に使用できなくなるリスクがあります。

セキュア・エレメントのデフォルト設定では、NVM書き込みをできる限り避けるようになっており、デバイスに鍵やファイルを恒久的に保管する場合にのみ、フラッシュ書き込み処理が行われます。

セキュア・オブジェクトまたは暗号オブジェクトの作成や削除により、フラッシュ書き込み処理が発生します。一時的セキュア・オブジェクトと暗号オブジェクトの場合、セキュア・オブジェクトの値を更新しても追加のフラッシュ書き込み処理は発生しません。永続的セキュア・オブジェクトの場合、セキュア・オブジェクトの値を更新するとフラッシュ書き込み処理が発生します。

ユーザーが認証オブジェクトで最大認証試行回数を設定する選択をすると、追加のフラッシュ書き込みが実行されます。その場合、認証が試行されるとそれがログに記録され、追加のフラッシュ書き込み処理が発生します。

前述した一般的ルールの例外が、ECモンゴメリ曲線25519が使用されている場合の共有シークレットの生成です。この場合、外部から提供される公開鍵がNVMにも保存されるため、共有シークレットが生成されるたびに、共有シークレットの生成に使用される外部の公開鍵を保存するための追加のNVM書き込み処理も発生します。

8.2 SE050Eの電力モード

SE050Eは、以下のような省電力動作をサポートしています。

- 「オフ」：このシナリオでは、Vinが供給されなくなります。結果として、まだNVメモリに保持されていないICの内部状態はすべて失われます。完全なスタートアップ・シーケンスを実行する必要があります。

- ENAピンを介した「ディープ・パワーダウン」：ENAピンがロー電位に設定されると、このモードに切り替わります。ICの観点から見た動作は、前述したパワーダウン・モードと同じです。過渡状態はすべて失われます。
- 「パワーダウン」：I²Cインターフェースを使用する場合は、I²Cリンクでコマンドを送信してデバイスをスリープ・モードに切り替えることができます。パワーダウン・モードでは、すべての過渡状態が保持され、次のAPDUとの通信を継続できます。GlobalPlatform APDU Transport Over I²Cプロトコルを使用する際は、[11]のS（RELEASE要求）ブロックと、CIPに含まれるPower Saving Timeout値 (PST) を参照してください。NXP SE05x T=1 Over I²Cプロトコルを使用する際は、[12]のSブロックEnd of APDUセッション要求を参照してください。
- アクティブ・モード：次のコマンドAPDUを待っていると、このモードに自動的に切り替わります。

SE050Eがアクティブに使用されていないときは、スタートアップ性能と省電力の要件に応じて、前述したいずれかのモードが選択される必要があります。

8.2.1 アプリケーション回路：基本的なI²Cの使用

使用されている構成：

- ホストからSE050EまでI²Cを使用
- SE050EはV$_{cc}$を介してオフにする
- 非接触およびI²Cコントローラは以下のアプリケーション回路図には含まれていない
- V$_{cc}$ピンをV$_{out}$ピンの代わりにV$_{in}$ピンに接続することもできる。その場合、V$_{out}$ピンは接続されない

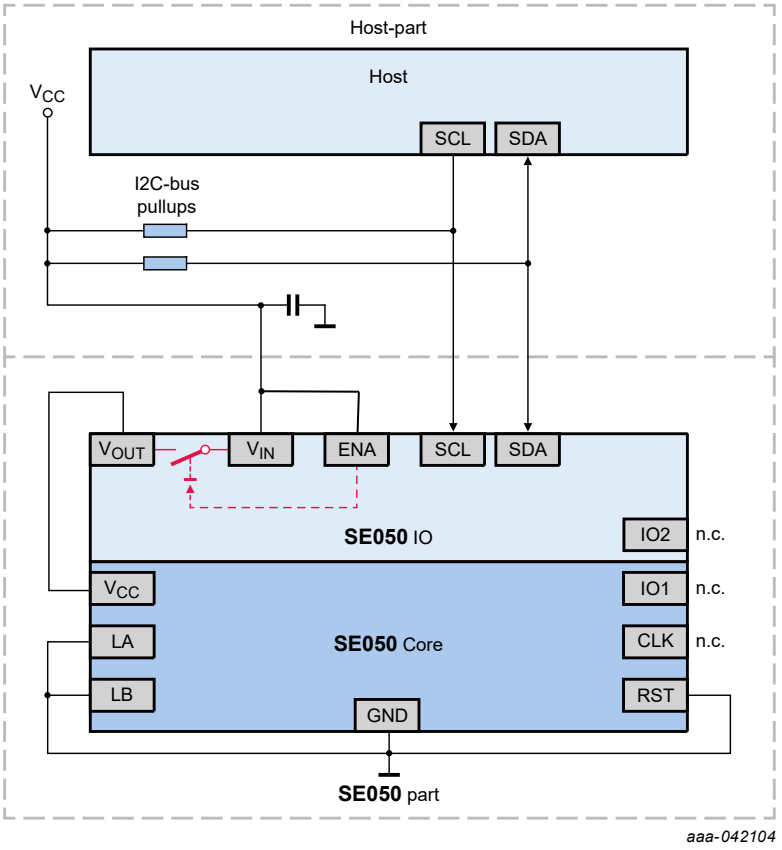

図12.アプリケーション回路：I²C

8.2.2 アプリケーション回路：ディープ・パワーダウンを使用したI²C

使用されている構成：

- ホストからSE050EまでI²Cを使用
- SE050Eはディープ・パワーダウン・モード（ENAピンがロー）を使用してオフにする
- 非接触およびI²Cコントローラは以下のアプリケーション回路図には含まれていない

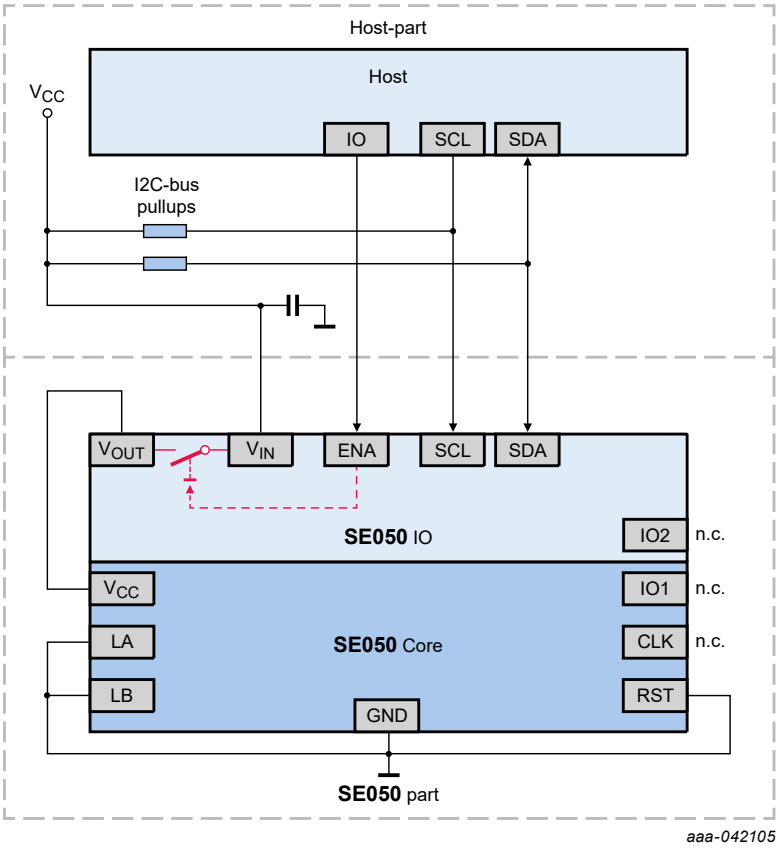

図13.アプリケーション回路：ディープ・パワーダウンを使用したI²C

V_{out}とV_{cc}間の接続部に追加のコンデンサは配置しません。

8.2.3 アプリケーション回路：I²Cコントローラ（ディープ・パワーダウンを使用）

使用されている構成：

- ホストからSE050EまでI²Cを使用
- SE050Eはディープ・パワーダウン・モード（ENAピンがロー）を使用してオフにする
- I²Cコントローラ・インターフェースを接続。以下のアプリケーション回路図では、SE050EのV_{out}から外部センサに給電
- 非接触およびI²Cコントローラは以下のアプリケーション回路図には含まれていない

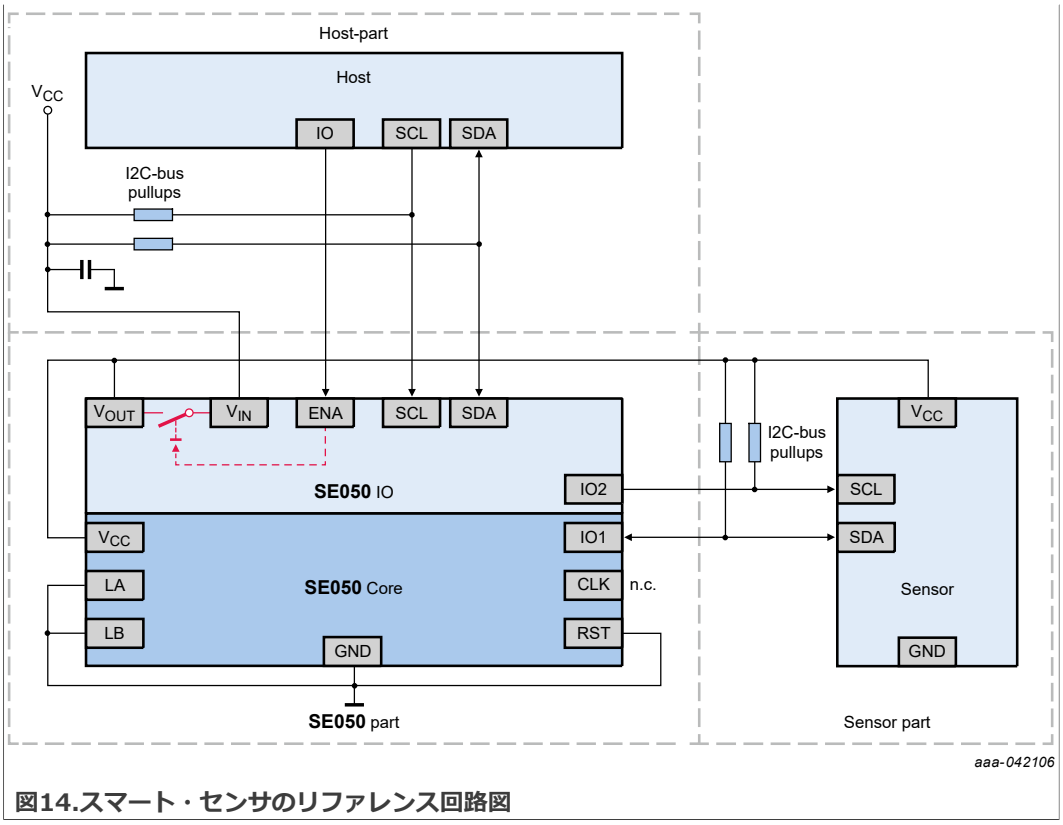

図14.スマート・センサのリファレンス回路図

9 参考資料

[1] アプリケーション・ノート：SE05x IoTアプレットAPDU仕様、AN12543。
[2] アプリケーション・ノート：SE050の設定、AN12436。
入手先： https://www.nxp.jp/docs/en/application-note/AN12436.pdf
[3] アプリケーション・ノート：SE05xによるAzure IoT Hubへのセキュアな接続、AN12402。
入手先： https://www.nxp.jp/docs/en/application-note/AN12402.pdf
[4] アプリケーション・ノート：SE05xによるAWS IoT Coreへのセキュアな接続、AN12404。
入手先： https://www.nxp.jp/docs/en/application-note/AN12404.pdf
[5] アプリケーション・ノート：SE05xによるOEM Cloudへのセキュアな接続AN12400。
入手先： https://www.nxp.jp/docs/en/application-note/AN12400.pdf
[6] アプリケーション・ノート：SE05xによるGCPへのセキュアな接続、AN12401。
入手先： https://www.nxp.jp/docs/en/application-note/AN12401.pdf
[7] アプリケーション・ノート：SE05xによるIBM Watson IoTへのセキュアな接続、AN12403。
入手先：https://www.nxp.jp/docs/en/application-note/AN12403.pdf
[8] アプリケーション・ノート：SE05xによるデバイス間認証、AN12399。
入手先：https://www.nxp.jp/docs/en/application-note/AN12399.pdf
[9] RFC2119。入手先：https://tools.ietf.org/html/rfc2119
[10] GlobalPlatform Card Specificationバージョン2.3.1、GPC_SPE_034。
入手先： https://globalplatform.org/specs-library/card-specification-v2-3-1
[11] GlobalPlatform APDU Transport over SPI/I2C、バージョン1.0、GPC_SPE_172。
入手先： https://globalplatform.org/specs-library/apdu-transport-over-spi-i2cv1-0-gpc_spe_172
[12] NXP SE05x T=1 Over SPI/I2C仕様、UM11225。
入手先：https://www.nxp.jp/webapp/Download?colCode=UM11225
[13] アプリケーション・ノート：Visual Studioプロジェクト例を含むEdgeLock™ SE05xクイック・スタート・ガイド、AN12398。
入手先：https://www.nxp.jp/docs/en/application-note/AN12398.pdf

10 法的情報

10.1 定義

ドラフト — ドキュメントにおけるドラフト状態とは、内容がまだ内部審査中かつ正式な承認を必要とする状態にあり、変更や追加が生じる可能性があることを指します。NXP Semiconductorsは、ドラフト版のドキュメントに記載されている情報の正確性や完全性について、いかなる表明も保証も行わず、そのような情報を使用することによって生じる結果について、一切の責任を負いません。

10.2 免責事項

限定的な保証と責任 — このドキュメントに記載されている情報は、正確かつ信頼できると判断された情報です。ただし、NXP Semiconductorsは、そのような情報の正確性や完全性について、明示、黙示を問わずに、いかなる表明も保証も行わず、そのような情報を使用することによって生じる結果について、一切の責任を負いません。NXP Semiconductorsは、このドキュメントの内容がNXP Semiconductors社外の情報源から提供されたものである場合、その情報について、いかなる責任も負いません。

NXP Semiconductorsは、間接的損害、付随的損害、懲罰的損害、特別損害、結果的損害（利益の損失、貯蓄の損失、事業の中断、製品の撤去や交換に関連する費用、または再加工の料金を含むが、これらに限定されない）について、その損害が不法行為（過失を含む）、保証、契約の不履行、その他の法理論に基づくか否かを問わず、いかなる場合も一切の責任を負いません。

理由の如何を問わず、お客様がいかなる損害を被ったとしても、ここに記載された製品に関するお客様へのNXP Semiconductorsの累積責任は、NXP Semiconductorsの商業販売に関する契約条件に従って制限されます。

変更を加える権利 — NXP Semiconductorsは、このドキュメントで公開された情報（仕様や製品の説明を含むが、これらに限定されない）に、事前に通知することなく、いつでも変更を加える権利を留保します。このドキュメントは、このドキュメントの発行前に提供されたすべての情報に優先し、それらに代わるものとします。

使用への適合性 — NXP Semiconductors製品は、生命維持、ライフ・クリティカル、またはセーフティ・クリティカル・システム/装置での使用、およびNXP Semiconductors製品の不具合や誤動作によって人身傷害、死亡、または重大な物的損害や環境損害が生じることが十分予想できるアプリケーションでの使用に適した製品として設計、認可、保証されているものではありません。NXP Semiconductorsおよびそのサプライヤは、前述した装置またはアプリケーションへのNXP Semiconductors製品の導入や使用について、いかなる責任も負わず、お客様が自らの責任でそのような導入や使用を行うものとします。

アプリケーション — 各製品に関連してここに記載されているアプリケーションは、説明のみを目的としたものです。NXP Semiconductorsは、そのようなアプリケーションが追加のテストや変更なしで特定用途に適したアプリケーションになるという表明も保証も行いません。

お客様は、NXP Semiconductors製品を使用したアプリケーションと製品の設計および運用について責任を負うものとし、NXP Semiconductorsは、アプリケーションやお客様の製品設計についてのいかなる支援にも、一切の責任を負いません。NXP Semiconductors製品が、お客様の計画中のアプリケーションや製品のほか、お客様の外部顧客が計画している適用や使用に適しているかどうかの判断については、お客様が全責任を負います。お客様は、自社のアプリケーションや製品に関連するリスクを最小限に抑えるための、適切な設計および運用上の安全対策を提供する必要があります。

NXP Semiconductorsは、お客様のアプリケーションや製品、またはお客様の外部顧客による適用や使用に何らかの不足や不履行がある場合、それに基づいたいかなる不履行、損害、費用、または問題についても、一切の責任を負いません。お客様は、アプリケーションや製品、またはお客様の外部顧客による適用や使用の不履行を回避するため、NXP Semiconductors製品を使用するお客様のアプリケーションと製品に必要なすべてのテストを実施する責任を負います。この点において、NXPはいかなる責任も負いません。

商業販売の契約条件 — NXP Semiconductors製品は、書面での有効な個別契約において別段の合意がない限り、http://www.nxp.jp/profile/termsで公開されている商業販売の一般契約条件に従って販売されます。個別契約が締結されている場合は、各契約の契約条件のみが適用されます。NXP Semiconductorsは、お客様によるNXP Semiconductors製品の購入に関して、お客様の一般契約条件を適用することに、明示的に異議を唱えます。

輸出管理 — このドキュメントとここに記載されている各項目は、輸出管理規則の対象となる可能性があります。輸出には管轄当局からの事前承認が必要になることがあります。

製品の評価 — 本製品は、「現状有姿」かつ「瑕疵を問わない」条件で、評価のみを目的に提供されます。NXP Semiconductorsとその関連会社およびサプライヤは、非侵害、商品性、特定目的への適合性の黙示的保証を含む（ただしこれらに限定されない）すべての明示的、黙示的、または法定の保証を明示的に否認します。本製品の品質、またはその使用や運用によって生じるリスク全体の責任は、お客様が負います。

NXP Semiconductorsとその関連会社またはサプライヤは、製品の使用または使用不能によって生じる特別損害、間接的損害、結果的損害、懲罰的損害、または付随的損害（事業の損失、事業の中断、使用不能による損失、データまたは情報の損失などの損害を含むが、これらに限定されない）について、たとえそのような損害の可能性について助言を受けていたとしても、不法行為（過失を含む）、厳格責任、契約の不履行、保証の不履行、その他の法理論に基づくか否かを問わず、いかなる場合も一切の責任を負いません。

理由の如何を問わず、お客様がいかなる損害（前述したすべての損害とすべての直接的損害または一般損害を含むが、これらに限定されない）を被ったとしても、前述したすべての損害に対するNXP Semiconductorsとその関連会社およびサプライヤの全責任、およびお客様の排他的な救済措置は、合理的な信頼に基づきお客様が実際に被った損害として、お客様が製品に対して実際に支払った金額または5ドル（5.00米ドル）のうち、いずれか高い金額までに制限されます。前述の制限、除外、免責事項は、救済措置がその本来の目的を達成できない場合でも、適用法によって認められる最大限の範囲に適用されます。

翻訳 — 法的情報を含む非英語（翻訳）版のドキュメントは参照用です。翻訳版と英語版に相違がある場合は、英語版が優先されます。

セキュリティ — お客様は、すべてのNXP製品が未確認の脆弱性にさらされる可能性があること、あるいは確立されたセキュリティ基準または仕様を既知の制限の下でサポートしている場合があることを理解しているものとします。お客様は、アプリケーションと製品のライフサイクル全体を通して、お客様のアプリケーションと製品に対する、前述した脆弱性の影響を軽減する設計および運用を行う責任を負います。お客様の責任は、お客様のアプリケーションでの使用を目的とした、NXP製品でサポートされる他のオープンソース・テクノロジや独自技術にも及びます。NXPは、いかなる脆弱性についても、一切の責任を負いません。お客様は、NXPによるセキュリティの更新を定期的に確認し、適切かつ継続的に管理する必要があります。

お客様は、NXPが提供する情報またはサポートに関わらず、目的とするアプリケーションの規則、規制、基準に最も適したセキュリティ機能を備える製品を選択し、自社の製品に関して最終的な設計上の判断を行い、その製品に関するすべての法律、規制、およびセキュリティに関連する要件の遵守に全責任を負うものとします。

NXPの製品セキュリティ・インシデント対応チーム (PSIRT)（問い合わせ先： PSIRT@nxp.com）は、NXP製品のセキュリティ上の脆弱性の調査、報告、および解決策の公開を管理しています。

10.3 商標

通知：記載されているすべてのブランド、製品名、サービス名、商標は、それぞれの所有者に帰属します。

NXP — 文字商標およびロゴは、NXP B.V.の商標です。

EdgeLock — NXP B.V.の商標です。

MIFARE — NXP B.V.の商標です。

表

図

目次

このドキュメントおよびここに記載されている製品についての重要なお知らせが、「法的情報」セクションに含まれていますので、ご注意ください。

詳細についてはvisit: http://www.nxp.jpをご覧ください。

リリース日：2022年8月22日
ドキュメントID：AN13483