注意：この日本語版文書は参考資料としてご利用ください。
最新情報は必ずオリジナルの英語版をご参照願います。

MICROCHIP

ECC608-TFLXWPC CryptoAuthentication™データシート

はじめに

ECC608-TFLXWPC は、ATECC608B 製品ファミリのプロビジョニング済みバージョンです。TrustFLEX セキュアエレメントは、Microchip 社の汎用プロビジョニング済みセキュリティ強化デバイス ファミリに属します。本デバイスのコンフィグレーションは、WPC (Wireless Power Consortium) Qi®規格バージョン 1.3 の認証要件を満たすよう設計されています。

ECC608-TFLXWPC のコンフィグレーションは、認証を行う Qi トランスミッタの基本的な認証要求を満たすよう定義されています。必要に応じて、2 つの WPC 証明書スロットを実装可能です。さらに、WPC インフラストラクチャ製品に TLS 認証を実装するための独自拡張機能またはセキュアブート機能が必要なユーザ向けに、追加のサポート機能を実装しています。アプリケーションに不要な未使用データスロットは、他の目的に柔軟に使う事ができます。これらのスロットのアクセスポリシーは、ECC608-TFLXWPC デバイスを注文する前に、Trust Platform Design Suite ツールにより設定されます。

本書は、ECC608-TFLXWPC に固有のスロットおよび鍵コンフィグレーション情報を提供します。これらの情報は、各 Data ゾーンスロットのアクセスポリシーを定義します。本書には、ECC608-TFLXWPC に関連するコマンドと I/O 動作情報のみを記載しています。「応用のための情報」では、アプリケーションの開発に役立つ Microchip 社のハードウェアおよびソフトウェア ツールを紹介すると共に、それらのツールに関連するリンクも提供します。

特長

- JIL で「高」評価 – JIL 文書『Application of Attack Potential to Smartcards and Similar Devices, Version 3.1』に対して確認済み
- 定義済み Configuration ゾーン(限られたオプションのみ選択可能)
- I^2C インターフェイス - I^2C アドレスは一度だけ変更可能
- WPC スロット 0 製造 CA と量産ユニット証明書をサポート
  - WPC 製造証明書認証局(CA) - 圧縮証明書と公開鍵
  - WPC 量産ユニット圧縮証明書
  - WPC 量産ユニット P-256 楕円曲線暗号(ECC)秘密鍵
- WPC スロット 1 または WPC スロット 2/3 独自拡張向けオプションサポート
- トランスミッタの迅速な WPC 再認証を可能にする WPC スロット ダイジェストをサポート
- TLS 認証のサポート
  - Google Cloud™、Amazon Web Services (AWS®)、Microsoft® Azure Cloud Services 等との連携が可能
  - TLS 署名者 – 圧縮証明書と公開鍵
  - TLS デバイス圧縮証明書
  - TLS デバイス P-256 ECC 秘密鍵
- I^2C 通信を保護する I/O 保護鍵スロット
- セキュアブートが可能(セキュアブート公開鍵は製造時にカスタマイズ可能)
- 8 ピン UDFN および 8 ピン SOIC パッケージ(数量は 2000 個単位)で提供

応用例

- WPC Qi 1.3 認証
- セキュア IoT TLS 1.2 および 1.3 接続
- セキュアブート/セキュア ファームウェア更新

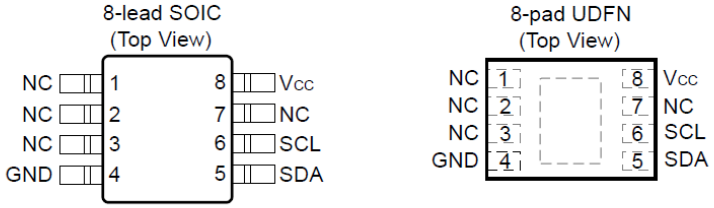
目次

1. ピンの構成と配置

表 1-1. ピン配置

ピン名	I²C デバイスの機能
NC	未接続
GND	グランド
SDA	I2C シリアルデータ
SCL	I2C シリアルクロック入力
VCC	電源

図 1-1. UDFN および SOIC パッケージのピン配置



Note: UDNF パッケージの底面露出パッドは、GND に接続する事を推奨します。

2. WPC (Wireless Power Consortium)

WPC (Wireless Power Consortium) は、携帯型機器向けのワイヤレス充電の開発に関する完全なエコシステムを定義しています。Qi 仕様のバージョン 1.3 から、5 W を超える電力レベルで充電を行う充電器に対して認証が要求されるようになりました。バージョン 1.3 では、携帯型機器を最大 15 W で充電可能です。全ての充電器は、認証なしで 5 W レベルの初期充電が可能です。5 W を超える充電を可能にするには認証動作が必要です。

これらの変更に対応するため、信頼の輪(Chain of Trust) が Qi エコシステムの一部として定義されています。この信頼の輪は以下の 3 つのレベルで構成されます。

1. **WPC ルート証明書:** ルート非公開鍵とルート証明書で構成される
2. **WPC 製造証明書:** ルート証明書の秘密鍵によって署名された製造証明書で構成される
3. **WPC 量産ユニット証明書:** WPC 製造証明書の秘密鍵によって署名された量産ユニット証明書で構成される

WPC 証明書は X.509 フォーマットに従います。WPC スロット 0 および 1 の証明書フォーマットは定義されています。WPC スロット 2 および 3 の証明書フォーマットは未定義であり、これらの証明書チェーンスロットはユーザが独自に使えます。

WPC ワイヤレス充電エコシステムに参加するには、WPC のメンバーである事が必要です。規格および WPC に関する詳細は、以下の WPC ウェブサイトでご覧ください。

www.wirelesspowerconsortium.com/.

2.1 WPC 関連の用語集

以下の用語の説明は、WPC Qi 認証規格に関する理解を助けるために記載しています。以下の内容は WPC 規格書内の情報に基づきますが、いかなる場合も規格書に記載されたオリジナルの内容が優先されます。

パワーレシーバ	パワー トランスミッタによって充電される装置です。この装置は、認証または充電制御のためにパワー トランスミッタと通信します。
パワー トランスミッタ	パワーレシーバと通信してパワーレシーバに電力を供給するための装置です。パワー トランスミッタはセキュア ストレージ サブシステムを内蔵します。
Qi	WPC によって策定された携帯型機器向けワイヤレス充電に関する規格の名称です。
RSID (Revocation Sequential Identifier)	RSID は WPC デバイスユニット証明書に保存される一意 ID です。この ID を使ってパワー トランスミッタを一意に識別し、それが非準拠である場合にトランスミッタの高電力動作を停止するか完全に動作を停止して安全な運用ができるようにします。
SSS (Secure Storage Subsystem)	ワイヤレス パワー トランスミッタを認証するためのセキュリティ情報を保存するストレージ デバイスです。これはセキュア エレメントまたはセキュア暗号デバイスであると見なせます。
WPC 製造者	WPC によって認証済み WPC パワー トランスミッタの製造を認可された企業または団体等。全ての WPC 製造者は WPC 製造者契約に署名する必要があります。
WPC 製造 CA	WPC によって WPC パワー トランスミッタ内で使用するセキュア ストレージ サブシステムの製造を認可された製造者です。Microchip 社は認可された製造 CA です。
WPC (Wireless Power Consortium)	Qi 規格に関連するワイヤレス充電の全ての側面を定義し、Qi 製品の認可および認証を行う標準化団体です。Qi に準拠するパワー トランスミッタおよびレシーバを製造するには WPC のメンバーである事が必要です。WPC の詳細は、以下の WPC ウェブサイトを参照してください。 www.wirelesspowerconsortium.com/.
WPC ルート認証局	WPC 証明書チェーンの起点です。全ての WPC 製造証明書は、WPC ルート認証局によって署名されます。

WPC スロット	WPC 認証仕様書は、スロットを「WPC 証明書チェーンを保持する要素」として定義しています。WPC 認証仕様書では 4 つのスロット (スロット 0～3) が使用可能とされ、スロット 0 は必ず WPC 証明書チェーンを保持する必要があり、必要に応じてスロット 1 も WPC 証明書チェーンとして使う事ができます。スロット 2 および 3 のフォーマットは定義されておらず、オプションの独自拡張用に提供されます。 本書では、WPC 証明書チェーンを指す意味で「WPC スロット」という用語を使います。これに対し、ECC608-TFLXWPC デバイス内のデータスロットを指す場合は「スロット」という用語を使います。
WPC スロット ダイジェスト	WPC スロットに保存された証明書チェーン全体の 32 バイト ダイジェストです。

3. EEPROM メモリの構成と Data ゾーン アクセスポリシー

EEPROM メモリは 1,400 バイトの総容量を持ち、以下のゾーンに分割されます。

表 3-1. ECC608-TFLXWPC の EEPROM ゾーン

ゾーン	概要	命名法
Configuration	以下を格納する 128 バイト(1,024 ビット) の EEPROM ゾーン • デバイス コンフィグレーション • スロット アクセスポリシー情報 • カウンタ値 • デバイスシリアル番号 • ロック情報 LockConfig バイトは設定済みです。Configuration ゾーンに直接書き込む事は一切できません。Configuration ゾーンは常に読み出し可能です。	Config[a:b] = Configuration ゾーンの 1 フィールドに含まれるバイトのレンジ
Data	1,208 バイト(9.7 K ビット)のゾーンが 16 個の読み出し専用または読み書き可能汎用メモリスロットに分割されます。Configuration ゾーン内のバイトによって定義されるアクセスポリシー情報により、各スロットへのアクセス方法が決まります。ECC608-TFLXWPC 内の各データスロットのアクセスポリシーは設定され、Configuration ゾーンによって定義されたスロット アクセスポリシーは完全な効力を有します。アクセスポリシーに応じて、そのスロットに対する読み出しまたは書き込みが可能かどうかが決まります。	Slot[YY] = Data ゾーンのスロット YY に保存された内容
OTP (One Time Programmable)	64 バイト(512 ビット) のゾーンが 2 つの 32 バイトブロックに分割されます。ECC608-TFLXWPC の OTP ゾーンには定義値が書き込み済みです。OTP ゾーンは変更できませんが、いつでも読み出せます。 詳細は 3.3 「ECC608-TFLXWPC の EEPROM OTP (One Time Programmable)ゾーン」を参照してください。	OTP[bb] = OTP ゾーン内の 1 バイト、 OTP[aa:bb] = OTP ゾーン内のバイトのレンジ

表 3-2. 本書内の用語の意味

本書内で使う用語の意味を下表に示します。

用語	意味
ブロック	1 ブロックは、特定メモリゾーン内の 256 ビット(32 バイト) 領域です。業界標準の SHA-256 文書でも「ブロック」という用語が使われますが、これはメッセージ入力の 512 ビット セクションを意味します。本書では、「ブロック」はハッシュ入力メッセージに言及する際にのみ使われます。
KeyID	KeyID は、鍵値を保持するために割り当てられたスロットの番号です。例えば、Key 1 (Key[1]と表記する場合もあり)は、Slot[1] に保存されます。16 個ある全てのスロットは鍵を保持できますが、平文読み出しを許可するよう設定されたスロットが暗号コマンドによって公開鍵または秘密鍵として使われる事は一般的にありません。
mode[b]	Mode パラメータのビット b を示します。
SRAM	入力および出力バッファと内部状態保存領域を格納します。ユーザが直接このメモリにアクセスする事はできません。
Word	1 ワードは、ブロックに対して読み書きする 4 バイトのデータです。ワードはデータアクセスの最小単位です。
LSB/MSB	最下位バイト/最上位バイト
LSb/MSb	最下位ビット/最上位ビット

3.1 ECC608-TFLXWPC の Configuration ゾーン

ECC608-TFLXWPC の Configuration ゾーンの大部分は固定されており、ユーザによる変更はできません。Microchip Trust Platform Design Suite を使っている場合、全てのコンフィグレーション情報はこのツールによって考慮されます。デバイスのコンフィグレーションに関連する情報を以下に示します。

デバイス コンフィグレーション情報

- 各デバイスのシリアル番号は一意であり、バイト[0:3, 8:12] に保存されます。バイト[0:1] は 0x01 0x23、バイト[8] は 0x01 です。その他の全てのバイトは一意です。
- 既定値の 7 ビット I^2C アドレスは 0x38 です。I^2C アドレスは、`UpdateExtra` コマンドを使って上書きできます。

重要: ECC608-TFLXWPC の既定値 I^2C アドレスは、プロビジョニング済みではない汎用 ATECC608B デバイスの既定値 I^2C アドレスとは異なります。

- I/O レベルは固定の参照電圧レベルに設定されているため、ホストプロセッサは ECC608-TFLXWPC の動作電圧よりも低電圧で駆動可能です。
- ウォッチドッグ タイマ(WDT) のタイムアウトは最大値(1.3 s) に設定されています。
- I/O 保護鍵の使用は、スロット 6 に保存された鍵により有効になります。
- ECC608-TFLXWPC では、スロット 3～6 とスロット 8～15 は個別に Lockable にするかどうか設定できます。
- ECC608-TFLXWPC では、SecureBoot で FullStore Digest モードが有効にされています。
- モノトニックカウンタはどの鍵にも割り当てられておらず、システムによって任意に使えます。
- ヘルステストに合格しなかったためにコマンド実行が失敗した場合、常に Health Test Failure ビットがクリアされます。失敗の症状が過渡的な物である場合、コマンドは再実行時にテストに合格する可能性があります。

3.1.1 Configuration ゾーン内の変更可能なバイト

Configuration ゾーンはロック済みであるため、このゾーン内のバイトに直接書き込む事はできません。しかし、一部のバイトは別のコマンドを使って変更できます。

SlotLocked ビット

ECC608-TFLXWPC では、スロット 3～6 とスロット 8～15 は個別に Lockable にするかどうか設定できます。Trust Platform Design Suite ツールにより、これらの各スロットは製造時に固定またはロック済みに設定できます。スロット 10～12 のグループとスロット 9、13、14 のグループは常に同じ設定にする必要があります。
Lockable に設定されたスロットは、`Lock` コマンドの SlotLock モードを使って、個々に 1 度だけロックできます。1 度ロックされたスロットは、変更もロックの解除もできなくなりますが、そのスロットに対して定義されているアクセスポリシーに基づいて使う事ができます。

SlotLocked バイトはバイト 88 と 89 に保存されます。初期状態では、これらのバイト内の全てのビットは「1」に設定されています。スロットをロックすると、そのスロットに対応するビットは「0」に設定されます。

I^2C アドレスの再定義

本デバイスは、I^2C アドレスが 1 度だけ変更できるように設定されています。`UpdateExtra` コマンドを使って Configuration ゾーン内のバイト 85 に新しい I^2C アドレスを書き込む事ができます。このバイトを非 0 値に設定すると、デバイス コンフィグレーションは既定値アドレスの代わりにバイト 85 の値を I^2C アドレスとして使います。新しいアドレスを有効にするには、このバイトを書き換えた後にデバイスの電源を 1 度遮断するか、デバイスをスリープモードに移行させる必要があります。

重要: I^2C アドレスを変更する必要がない場合、このバイト位置に既定値 I^2C アドレスを書き込む必要があります。

UserExtra バイト
UserExtra バイトは任意の目的で使えます。このバイトは、UpdateExtra コマンドを使って 1 度だけ更新できます。UserExtra バイトは、Configuration ゾーンのバイト 84 に配置されています。

Counter[0,1]
本デバイスはカウンタを使いませんが、カウンタは有効なままです。必要に応じ、システムはこれらのカウンタを使う事ができます。カウンタは 0 に初期化され、最大 2,097,151 までカウントできます。Counter コマンドにより、カウンタ値のインクリメントまたは読み出しが可能です。これらのカウンタは、本デバイスの他の機能とは無関係であり、システムによって自由に使う事ができます。カウンタ値は、Counter コマンドを使って読み出すか更新する事ができます。

3.2 Data ゾーンとアクセスポリシー

以下では、各スロットに割り当てられているアクセスポリシー情報について説明します。実際のアクセスポリシー情報は、EEPROM Configuration ゾーン内の SlotConfig および KeyConfig セクションに保存されます。各 Data ゾーンスロットには、2 つの Slot Configuration バイトと 2 つの Key Configuration バイトが割り当てられています。これらの 4 バイトにより、各スロットの「アクセスポリシー」が構成されます。スロットに保存されるデータのタイプは、そのスロットのアクセスポリシーによって決まります。

3.2.1 Data ゾーンのデータタイプ

以下では、ECC608- TFLXWPC のデータスロットに保存できる各種データタイプについて説明します。

3.2.1.1 秘密鍵

ECC 秘密鍵は、ECC セキュリティの基本構成要素です。これらの鍵は非公開かつ各デバイスに対して一意であり、読み取る事は決してできません。ECC 秘密鍵はプロビジョニング時に HSM によってランダムに生成され、ECC 秘密鍵として設定されたスロットでセキュアに保持されます。

TLS IoT 秘密鍵
これは IoT 接続用に使われるプライマリ認証鍵です。この鍵は恒久的であり、変更はできません。各デバイスは独自の一意秘密鍵を保有します。

この鍵は以下に対して有効です。

- 認証のための ECDSA 署名
- 鍵合意のための ECDHECDH 出力を暗号化する必要がある場合、I/O 保護鍵を最初にセットアップする必要があります。セットアップの詳細は 3.2.1.6 「I/O 保護鍵」を参照してください。

この秘密鍵は、対応する公開鍵と IoT TLS X.509 証明書を生成するための基本の鍵です。

WPC スロット 0/スロット 1 内の秘密鍵
これらの鍵は、WPC デバイス認証用に使われるプライマリ ECC 鍵です。通常、WPC スロット 0 内の鍵だけが使われます。

この鍵は以下に対して有効です。

- 認証のための ECDSA 署名

WPC スロット 0 と WPC スロット 1 内の各秘密鍵は、WPC X.509 量産ユニット証明書向けの対応する公開鍵を生成するための基本の鍵です。

3.2.1.2 ECC 公開鍵

公開鍵は常に ECC 秘密鍵と関連付けられます。各 ECC 秘密鍵は独自の一意公開鍵を持ちます。公開鍵はデバイス内に保存できる他、デバイススロットを適切に設定する事により GenKey コマンドを使って再生成する事ができます。ECC608-TFLXWPC では、以下の 7 種類の公開鍵を使用または生成できます。

- デバイススロット 0 および 1 は、WPC スロット 0 および 1 証明書チェーンに対応する WPC 量産ユニット証明書向けの ECC 秘密鍵を格納します。これらの各秘密鍵向けの公開鍵は、動作の検証用にいつでも生成および使用が可能です。
- デバイススロット 2 は、TLS IoT 認証向けの ECC 秘密鍵を格納します。この秘密鍵向けの公開鍵は、動作の検証用にいつでも生成および使用が可能です。
- デバイススロット 9 は、WPC スロット 0 製造 X.509 証明書向けの ECC 公開鍵を格納します。
- デバイススロット 8 は、WPC スロット 1 製造 X.509 証明書向けの ECC 公開鍵を格納します。この公開鍵は、このスロットの最初の 72 バイト内に保存されます。WPC スロット 1 が使われない場合、この鍵を別の用途で使う事ができます。別の用途でも使わない場合、この鍵は全く存在しなくても構いません。
- スロット 11 は、WX.509 IoT TLS 署名者証明書情報の一部として ECC 公開鍵を格納します。
- スロット 15 は、セキュアブート動作向けに使用可能な ECC 公開鍵を格納します。

3.2.1.3 証明書の保存

ECC608-TFLXWPC は、異なるユースケースに対応するために複数の証明書チェーンをサポートします。最大で 3 つの X.509 証明書チェーンをサポート可能です。通常 X.509 証明書は ECC608-TFLXWPC の 1 スロットのサイズより大きくなるため、圧縮フォーマットを使います。この方法は、動的な証明書情報をデバイスに保存してある程度の制限を課するため、部分的証明と呼ばれる手法よりも優れます。動的な情報とは、デバイスごとに異なると期待できる証明書内容です(例: 公開鍵、有効期限等)。
静的なデータは全てのデバイスで一定です。ファームウェアは、特定ユースケース向けの各 X.509 証明書を完全に再構成するために、テンプレートを使った証明書定義を持つ必要があります。完全な証明書は、動的データと静的データの組み合わせで構成されます。

ECC608-TFLXWPC では、IoT TLS ユースケースと WPC 認証ユースケースをサポートするために、2 種類の X.509 証明書が存在します。これらの各ユースケースは異なる X.509 フォーマットを使うため、ECC608-TFLXWPC は異なる圧縮証明書フォーマットを持ちます。WPC スロット 1 を使わずに WPC スロット 2 または WPC スロット 3 内の独自拡張を使う場合、タイプの異なる追加の証明書チェーンが必要になる場合があります。

3.2.1.3.1 TLS 証明書ストレージ

TLS X.509 証明書チェーンは、Microchip Trust&GO および TrustFLEX TLS 製品(具体的には ATECC608B-TNGTLS および ATECC608B-TFLXTLS) 向けに使われる証明書チェーンと同じです。

以下のアプリケーション ノートに、圧縮証明書のフォーマットが記載されています。

『ATECC Compressed Certificate Definition』

CryptoAuthLib ライブラリにも、TLS 圧縮証明書向けに使う atcacert モジュールが含まれています。

デバイス証明書
デバイス証明書は、実際の ECC608-TFLXWPC デバイス関する情報で構成されます。

署名者証明書
署名者証明書は、デバイス証明書に署名するために使われた署名者認証局に関連する情報で構成されます。完全な署名者証明書を再構成するには署名者公開鍵も必要です。

署名者公開鍵
署名者公開鍵は、署名者と圧縮された署名者証明書に関する情報を検証するために必要な公開鍵です。

表 3-3 に、証明書に関係する ECC608-TFLXWPC 内の全てのスロットを示します。

表 3-3. 証明書用スロット

スロット	概要
3	プライマリ秘密鍵: 公開鍵は、GenKey コマンドを Mode = 0x00 で使う事により、いつでも生成できます。
10	デバイス証明書: この証明書は圧縮フォーマットでこのスロットに保存されます。
11	署名者公開鍵

.....続き	
スロット	概要
12	署名者証明書: この証明書は圧縮フォーマットで保存されます。

ECC608-TFLXWPC 量産デバイスの場合、これらのスロットは恒久的(Permanent)またはロック可能(Lockable)として設定できます。初期開発を容易にするため、プロトタイプ デバイスのスロット 10～12 はロック可能(Lockable)に設定されます。

3.2.1.3.2 WPC 証明書ストレージ

WPC X.509 証明書チェーンは、WPC 1.3.0 認証仕様書内で文書化されています。この仕様書は、WPC の登録メンバーにのみ提供されます。Microchip 社が WPC X.509 証明書向けに使う圧縮フォーマットは、以前に Microchip 社が定義した TLS X.509 証明書向けフォーマットからの派生バージョンです。

WPC 証明書向けに使われる用語は、WPC 認証仕様によって使われている用語を反映したものです。

CryptoAuthLib ライブラリにも、WPC 圧縮証明書向けの atcawpccert モジュールが含まれています。

量産ユニット証明書
量産ユニット証明書は、セキュア ストレージ サブシステムに関連する情報で構成されます。量産ユニット証明書は、TLS 認証ユースケース向けに指定されるデバイス証明書と等価です。

製造者証明書
製造者証明書は製造者認証局に関連する情報で構成され、量産ユニット証明書に署名するために使われます。製造者証明書は、TLS 認証ユースケース向けに指定される署名者証明書と等価です。

製造者公開鍵
製造者公開鍵は、製造者と製造者圧縮証明書に関する情報を検証するために必要な公開鍵です。製造者公開鍵は、TLS 認証ユースケース向けに指定される署名者公開鍵と等価です。

表 3-4 に、WPC 証明書に関係する ECC608-TFLXWPC 内の全てのスロットを示します。

表 3-4. 証明書用スロット

WPC スロット 0	WPC スロット 1	概要
0	1	プライマリ WPC 秘密鍵公開鍵は、GenKey コマンドを Mode = 0x00 で使う事により、いつでも生成できます。
4	8	製造者証明書または量産ユニット証明書向けに必要な追加データです。
5	8	量産ユニット証明書向けに必要な RSID です。
13	8	量産ユニット証明書です。この証明書は WPC 圧縮フォーマットで保存されます。
9	8	署名者公開鍵
14	8	製造者証明書この証明書は WPC 圧縮フォーマットで保存されます。

ECC608-TFLXWPC 量産デバイスの場合、これらのスロットは恒久的(Permanent)またはロック可能(Lockable)として設定できます。初期開発を容易にするため、プロトタイプ デバイスのスロット 4、5、8、9、13、14 はロック可能(Lockable) に設定されます。

3.2.1.4 WPC スロット ダイジェスト

WPC 認証仕様は、証明書を使った完全な認証に加えて、WPC スロット 0 または WPC スロット 1 に関連するダイジェストを単純に比較する簡易な認証方法を許容します(簡易法を使うには、そのように定義する必要があります)。この方法を使うには、あらかじめ完全な認証を行って WPC スロットのダイジェストを計算して保存しておく必要があります。

ダイジェストの値は、WPC スロット全体に対して SHA-256 として計算された 32 バイト値です。仕様は、定義された各 WPC スロット向けに 1 つのダイジェストを許容します。ECC608-TFLXWPC は、2 つのダイジェスト向けのストレージを備えています。デバイススロット 3 が WPC スロット 0 向けに使われます。WPC スロット 1 のダイジェストはスロット 8 [288:319] に保存されます。

3.2.1.5 セキュアブート

ECC608-TFLXWPC では、SecureBoot コマンドは有効となっています。このため、システムは完全なブートを実行する前に、ブートローダを介してファームウェアを暗号論的に検証できます。この機能を使うと、新しいファームウェア イメージをロードする前に検証する事もできます。

セキュアブート機能を使う前に、P-256 ファームウェア署名鍵を確立する必要があります。秘密鍵は、ファームウェア イメージの署名用に、ファームウェア開発者が保有します。公開鍵を「セキュアブート公開鍵」スロットに書き込み、スロットをロックする事で鍵を恒久的(Permanent)とする必要があります。

ECC608-TFLXWPC の場合、使用を許可する前に有効なセキュアブートを要求するよう、TLS プライマリ秘密鍵と WPC スロット 0 および WPC スロット 1 の ECC 鍵を有効にする事もできます。この機能を有効にする方法は、3.2.4 「セキュアブート オプション」を参照してください。

詳細な説明は 4.2.3 「SecureBoot コマンド」を参照してください。

セキュアブートを実装するには、複数のデータスロットが必要です。

セキュアブート ダイジェスト

セキュアブート ダイジェストは、ファームウェア アプリケーション コードに対して計算される 32 バイトの SHA-256 ダイジェストです。このダイジェストは、ファームウェアを更新するたびに更新する必要があります。ECC608-TFLXWPC の場合、ダイジェストはスロット 7 に保存されます。

セキュアブート公開鍵
セキュアブート公開鍵は、セキュアブート ダイジェストと署名を有効にするための検証機能向けに使われます。セキュアブート公開鍵はスロット 15 に保存されます。

3.2.1.6 I/O 保護鍵

Verify、ECDH、SecureBoot、KDF コマンドでは、オプションにより I/O 保護機能を使って一部のパラメータを暗号化し、一部のレスポンスを検証できます(MAC コマンドによる)。これは、物理的 I^2C バス上での中間者攻撃を防ぐために役立ちます。しかし、この機能を使う前に、MCU と ECC608-TFLXWPC は一意の I/O 保護鍵を生成して保存する事で、原則的に互いにペアリングする必要があります。ペアリング処理は、最初のブート時に発生する必要があります。

I/O 保護鍵の生成:

1. MCU は random コマンドを使ってランダムな 32 バイト I/O 保護鍵を生成します。
2. MCU は I/O 保護鍵を MCU 内部のフラッシュに保存します。
3. MCU は I/O 保護鍵を I/O 保護鍵スロットに書き込みます。
4. MCU はそのスロットをロックする事で、I/O 保護鍵を恒久的とします。

ペアリングを確認するため、MCU は MAC コマンドを使ってチャレンジを I/O 保護鍵に対して発行し、フラッシュに保存されている I/O 保護鍵と ECC608-TFLXWPC 内の I/O 保護鍵が一致するか検証します。

3.2.1.7 汎用データストレージ

全てのスロットは定義された目的向けに設定されますが、すべての機能が必要なわけではありません。WPC スロット 1 情報が不要である場合、スロット 4 とスロット 8 は汎用データストレージとして使えます。TLS 認証ユースケースが不要である場合、スロット 10～12 は汎用データストレージとして使えます。データはプロビジョニング中に書き込むか、スロットを Lockable のままにしておいてフィールドで書き込む事ができます。

3.2.2 スロット設定の用語

以下に、設定オプションの説明に使う用語をアルファベット順に記載します。

用語	意味
AES Key:	AES コマンドの鍵ソースと使えるスロットです。ECC608-TFLXWPC では、AES 鍵は 128 ビット幅を持ちます。

用語	意味
Always Write:	Write コマンドを使っていつでも平文で書き込めるスロットです。
Clear Read:	パブリックである(秘密ではない)と見なされ、Read コマンドを使ってその内容を平文で読み出せるスロットです。
ECDH:	楕円曲線ディフィー ヘルマン(Elliptic Curve Diffie Hellman) ECDH コマンドで使える秘密鍵です。
Encrypted Write:	スロットに書き込むには、指定された書き込み鍵に基づく暗号化書き込みを使う必要があります。
Ext Sign:	外部(任意の)メッセージを署名するために使える秘密鍵です。
Int Sign:	GenKey または GenDig コマンドによって生成された内部メッセージに署名するために使える秘密鍵です。デバイス内部の鍵と設定を証明するために使われます。
Lockable:	将来のある時点でロックできるスロットです。1 度ロックしたスロットの内容は変更できません(読み出し/使用のみ可能)。
No Read:	秘密であると見なされ、Read コマンドを使って読み出す事ができないスロットです。秘密鍵と対称秘密鍵は常に「No Read」として設定する必要があります。
No Write:	Write コマンドを使って変更できないスロットです。
Permanent:	恒久的で変更不可能な秘密鍵です。この秘密鍵は工場でのプロビジョニング中に内部生成されます。
Updatable:	後でランダムに内部生成された秘密鍵により上書き可能な秘密鍵です。初期値は工場でのプロビジョニング中に内部生成されます。
Validated:	公開鍵はペアレント公開鍵によって有効にされた後に Verify コマンドでのみ使えます。

3.2.3 ECC608-TFLXWPC のスロット設定のまとめ

ECC608-TFLXWPC は、各種の用途向けに設定される 16 個のスロットを備えています。ECC608-TFLXWPC におけるこれらのスロットの設定と推奨ユースケースを表 3-5 に示します。

表 3-5. スロット設定

スロット	ユースケース	概要	プライマリ コンフィグレーション
0	WPC スロット 0 認証	WPC スロット 0 プライマリ ECC 認証鍵	Permanent、Ext Sign、 Not Readable、 セキュアブート(オプション)
1[1]	WPC スロット 1 認証	WPC スロット 1 プライマリ ECC 認証鍵	Permanent、Ext Sign、 Not Readable、 セキュアブート(オプション)
2	TLS 認証	プライマリ TLS ECC 認証鍵	Permanent、Ext Sign、ECDH、 Not Readable、 セキュアブート(オプション)
3	WPC スロット 0 認証	WPC スロット 0 証明書チェーン ダイジェスト	Permanent または Writable かつ Slot Lockable、Clear Text Read (アクセスポリシーに依存)
4	WPC スロット 0 認証	WPC スロット 0 追加情報	Permanent または Writable かつ Slot Lockable、Clear Text Read (アクセスポリシーに依存)
5	WPC スロット 0 認証	WPC スロット 0 追加情報	Permanent または Writable かつ Slot Lockable、Clear Text Read (アクセスポリシーに依存)
6	I/O 保護鍵	特定コマンドの I^2C バス通信(I/O)を保護するために使う鍵 (使用前に設定する必要があります)	Permanent または Writable かつ Slot Lockable、Never Read (アクセスポリシーに依存)

.....続き

スロット	ユースケース	概要	プライマリ コンフィグレーション
7	セキュアブート	セキュアブート ダイジェスト向けのストレージ (これは内部機能であり、読み書きはできません)	No Read、No Write
8[2]	WPC スロット 1 認証	WPC スロット 1 情報公開鍵、証明書、スロットダイジェスト向けストレージ	Clear Text Read、Writable または Lockable (アクセスポリシーに依存)
9	WPC スロット 0 認証	WPC スロット 0 製造者公開鍵	Permanent、Clear Read、No Write または Writable (アクセスポリシーに依存)
10	TLS 認証	CryptoAuthentication™ 圧縮フォーマットの TLS デバイス圧縮証明書	Permanent、Clear Read、No Write または Writable (アクセスポリシーに依存)
11	TLS 認証	デバイス証明書に署名する CA (署名者)向け TLS 公開鍵	Clear Read、No Write または Writable (アクセスポリシーに依存)
12	TLS 認証	CryptoAuthentication™圧縮フォーマットでのデバイス証明書の CA (署名者)証明書向け TLS 証明書	Clear Read、No Write または Writable (アクセスポリシーに依存)
13	WPC スロット 0 認証	WPC スロット 0 圧縮デバイス証明書	Permanent、Clear Read、No Write または Writable (アクセスポリシーに依存)
14	WPC スロット 0 認証	WPC スロット 0 圧縮製造者証明書	Permanent、Clear Read、No Write または Writable (アクセスポリシーに依存)
15	セキュアブート	セキュアブート公開鍵	Permanent または Writable かつ Lockable、Clear Text Read

Note:

1. このスロットは ECC 秘密鍵向けに予約済みです。WPC スロット 1 が不要である場合、このスロットは WPC スロット 2 で使う秘密鍵を格納するか、その他の用途で使う事ができます。
2. WPC スロット 1 がアプリケーション内で使われない場合、このスロットは WPC スロット 2 または 3 情報向けに使う事ができます。このスロットを公開鍵または証明書情報向けに使う場合、このスロットをロックする事を推奨します。その他の WPC スロットが不要である場合、このスロットは汎用データの保存用に使えます。

3.2.4 ECC608-TFLXWPC スロット アクセスポリシーの詳細

ECC608-TFLXWPC の WPC 向け既定値コンフィグレーションは、WPC スロット 0 に関連する情報のみを使います。WPC スロット 0 に関連するデバイススロット内の全ての情報(スロット 3 内に保存される WPC スロット 0 ダイジェストを除く) は、認証手続きまたは証明書チェーンの一部として必須です。

注意: WPC スロット 0 の既定値設定以外の機能を使う場合、事前に Microchip 社に確認してください。全ての機能がプロビジョニング システムに初期実装されているわけではありません。

ECC608-TFLXWPC は、以下の柔軟性を提供します。

1. スロットを恒久的にロックするかロック可能(Lockable)なままにするか
2. セキュアブートを鍵および持続性ラッチに結び付けるかどうか

スロットロック オプション
スロットロック オプションは、各スロットで以下のどちらかに設定できます。

Slot Lockable: このスロットロック オプションに設定されたスロットは、初期製造後の任意時点でエンドユーザによるロックが可能です。これにより、本デバイスが Microchip 社から出荷された後の製造工程中に鍵

を設定できます。あるいは、エンドユーザによる鍵の設定も可能です。スロットは Lock コマンドを使ってロックできます。スロットが 1 度ロックされると、その中のデータは 2 度と変更できなくなります。

Permanent Lock: デバイスが Microchip 社の工場から出荷された後に、恒久的にロックされたスロットを変更する事は決してできません。これらのデバイスのプロビジョニングに先立ち、正しいデータと鍵を Microchip 社に提供する必要があります。

セキュアブート オプション

セキュアブート アクセスポリシーは、セキュアブートが成功する前のコマンドの実行を制限するためのオプションを提供します。コマンドアクセスを一切制限しない事も可能です。スロット 0、1、2 内の ECC 秘密鍵は、ほとんどのコマンドでの使用に対してこれらの鍵が認証される前にセキュアブートを要求するよう設定できます。この機能を使うには、セキュアブート コンフィグレーション設定と鍵コンフィグレーション値に対する変更が必要です。これらの設定変更は、セキュアブートが成功した時に持続性ラッチを設定します。スロット 0 のアクセスポリシーを変更すると、鍵の使用は設定される持続性ラッチに結び付けられます。

持続性ラッチの動作

持続性ラッチは、アイドルおよびスリープモード中も状態を維持します。このため、電源投入後にセキュアブート動作を 1 回実行するだけで済みます。デバイスの電源電圧が最低許容レベルを下回ると持続性ラッチはリセットされ、新たにセキュアブートを実行する必要があります。

プロトタイプ デバイス

プロトタイプ デバイスの特定の既定値設定は変更できません。既定値設定により、全てのスロットのオプションはロック可能(Lockable) に設定されています。このため、アプリケーションによって鍵を再設定する事で、ソフトウェアの開発時に最大限の自由度が得られます。最終的な設定は、この方法で設定する必要はありません。プロトタイプ デバイスでは、セキュアブート オプションを利用できません。このオプションは、量産デバイス向けにのみ選択可能です。プロトタイプ デバイスでは I^2C インターフェイスのみが利用可能です。

スロット設定の詳細

以下の各表に、本デバイスの各スロットにおけるスロットと鍵の詳細な設定を示します。各スロットに対して適用可能なコマンドとコマンドモードも記載しています。これらの表は、ECC608-TFLXWPC で利用可能な全ての鍵およびスロット設定値をスロットごとに示しています。

表 3-6. スロット 0 の設定情報

スロット	設定値	有効機能
0	**オプション 1: Not Connected to Persistent Latch**	
	鍵:	**WPC スロット 0 ECC 秘密鍵** • P-256 NIST ECC 秘密鍵を格納します。 • 対応する公開鍵はいつでも生成できます。 • ランダムノンスが必要です。
	スロット:	• このスロットは秘密です。 • 外部メッセージに署名できます。
	オプション 2: Connected to Persistent Latch	
	鍵:	オプション 1 の機能に加えて、 • この鍵はセキュアブートの実行後にのみ使用可能です。
	スロット:	オプション 1 と同じです。

表 3-7. スロット 1 の設定情報

スロット	設定値	有効機能
1	**オプション 1: Not Connected to Persistent Latch**	
	鍵:	**WPC スロット 1 ECC 秘密鍵** • P-256 NIST ECC 秘密鍵を格納します。 • 対応する公開鍵はいつでも生成できます。 • ランダムノンスが必要です。
	スロット:	• スロットは秘密です。 • 外部メッセージに署名できます。
	オプション 2: Connected to Persistent Latch	
	鍵:	オプション 1 の機能に加えて、 • この鍵はセキュアブートの実行後にのみ使用可能です。
	スロット:	オプション 1 と同じです。

表 3-8. スロット 2 の設定情報

スロット	設定値	有効機能
2	**オプション 1: Not Connected to Persistent Latch**	
	鍵:	**TLS セッション秘密鍵** • P-256 NIST ECC 秘密鍵を格納します。 • 対応する公開鍵はいつでも生成できます。 • ランダムノンスが必要です。
	スロット:	• スロットは秘密です。 • 外部メッセージに署名できます。 • ECDH コマンドで使えます。
	オプション 2: Connected to Persistent Latch	
	鍵:	• オプション 1 と同じです。 • 持続性ラッチ ディセーブル オプションは有効です。
	スロット:	• オプション 1 と同じです。

表 3-9. スロット 3 の設定情報

スロット	設定値	有効機能
3	**オプション 1: Permanent Lock**	

.....続き

スロット	設定値	有効機能
	鍵:	**WPC スロット 0 ダイジェスト** • WPC スロット 0 証明書チェーンの 32 ビット ダイジェストを格納します。 • このスロットは恒久的にロックされます。
	スロット:	• 常に平文で読み出し可能です。 • 固定
	オプション 2: Slot Lockable and Writable	
	鍵:	• スロットは Lockable です。
	スロット:	• 平文でデータを書き込めます。 • 常に読み出し可能です。

表 3-10. スロット 4 の設定情報

スロット	設定値	有効機能
4	**オプション 1: Permanent Data**	
	鍵:	**WPC スロット 0 その他のデータ** • WPC スロット 0 その他のデータを保存するために使います。 • スロットは固定です。
	スロット:	• 常に平文で読み出し可能です。 • 固定
	オプション 2: Slot Lockable and Writable	
	鍵:	• WPC スロット 0 その他のデータを保存するために使います。 • スロットは Writable です。
	スロット:	• 常に平文で読み出し可能です。 • スロットは Lockable です。

表 3-11. スロット 5 の設定情報

スロット	設定値	有効機能
5	**オプション 1: Permanent Data**	
	鍵:	**WPC スロット 0 その他のデータ(続き)** • WPC スロット 0 その他のデータを保存するために使います。 • スロットは固定です。
	スロット:	• 常に平文で読み出し可能です。 • 固定
	オプション 2: Slot Lockable and Writable	
	鍵:	• WPC スロット 0 その他のデータを保存するために使います。 • スロットは Writable です。
	スロット:	• 常に平文で読み出し可能です。 • スロットは Lockable です。

表 3-12. スロット 6 の設定情報

スロット	設定値	有効機能
6	**オプション 1: Slot Lockable**	
	鍵:	**I/O 保護鍵** • SHA-256 対称鍵またはその他のデータを格納できます。I/O 保護鍵を使わない場合、このスロットはその他のデータ用に使えます。 • この鍵を使うにはランダムノンスが必要です。 • このスロットは個別にロックできます。
	スロット:	• 平文でデータを書き込めます。 • このスロットの内容は秘密であり、読み出しはできません。 • このスロットは CheckMac Copy コマンド向けに使えません。
	オプション 2: Permanent Lock	
	鍵:	• スロットが恒久的にロックされる事を除き、オプション 1 と同じです。
	スロット:	• スロットが書き込めない事を除き、オプション 1 と同じです。

重要: 一般的に、スロット 6 に保存された I/O 保護鍵は Slot Lockable オプションのままにする必要があります。ほとんどの場合、I/O 保護鍵は各デバイスで一意です。ユースケースによっては、全てのデバイスで同じ I/O 保護鍵を使います。その場合、Permanent Lock オプションを選択できます。

表 3-13. スロット 7 の設定情報

スロット	設定値	有効機能
7	鍵:	**セキュアブート ダイジェスト** • このスロットは、その他のデータ向けに割り当てられています。
	スロット:	• このスロットは直接読み書きできません。 • このスロットは秘密であり、MAC コマンドで使う事はできません。 • このスロットは CheckMac Copy コマンド向けに使えません。

表 3-14. スロット 8 の設定情報

スロット	設定値	有効機能
8	**オプション 1: Slot Lockable**	
	鍵:	**WPC スロット 1 データ** • このスロットは、WPC スロット 1 データ向けに割り当てられます。 • スロットは Lockable です。
	スロット:	• このスロットに対して平文の読み書きが可能です。 • このスロットは CheckMac Copy コマンド向けに使えません。
	オプション 2: Permanent Lock	
	鍵:	• スロットが恒久的にロックされる事を除き、オプション 1 と同じです。
	スロット:	• スロットが書き込めない事を除き、オプション 1 と同じです。

表 3-15. スロット 9 コンフィグレーション情報

スロット	設定値	有効機能
9	**オプション 1: Permanent Lock**	
	鍵:	**WPC スロット 0 公開鍵** • このスロットは ECC 鍵向けに定義されます。 • ECC 鍵は公開鍵です。
	スロット:	• データを上書きする事はできません。 • 平文でデータを読み出せます。
	オプション 2: Slot Lockable *Note: これはプロトタイプ デバイス向けの設定です。*	
	鍵:	• オプション 1 の全ての機能 • スロットは Lockable です。
	スロット:	• スロットが書き込み可能である事を除き、オプション 1 と同じです。

表 3-16. スロット 10 の設定情報

スロット	設定値	有効機能
10	**オプション 1: Permanent Lock**	
	鍵:	**デバイス圧縮証明書** • このスロットは、その他のデータの保存用として定義されます
	スロット:	• データを上書きする事はできません。 • 平文でデータを読み出せます。
	オプション 2: Slot Lockable *Note:これはプロトタイプ デバイス向けの設定です。*	
	鍵:	• オプション 1 の全ての機能 • スロットは Lockable です。
	スロット:	• スロットが Writable である事を除き、オプション 1 と同じです。

表 3-17. スロット 11 の設定情報

スロット	設定値	有効機能
11	**オプション 1: Permanent Lock**	
	鍵:	**署名者公開鍵** • このスロットは ECC 鍵向けに定義されます。 • ECC 鍵は公開鍵です。
	スロット:	• データを上書きする事はできません。 • 平文でデータを読み出せます。
	オプション 2: Slot Lockable *Note:これはプロトタイプ デバイス向けの設定です。*	
	鍵:	• オプション 1 の全ての機能 • スロットは Lockable です。
	スロット:	• スロットが Writable である事を除き、オプション 1 と同じです。

表 3-18. スロット 12 の設定情報

スロット	設定値	有効機能
12	**オプション 1: Permanent Lock**	
	鍵:	**署名者圧縮証明書** • このスロットは、その他のデータの保存用として定義されます
	スロット:	• データを上書きする事はできません。 • 平文でデータを読み出せます。
	オプション 2: Slot Lockable *Note:これはプロトタイプ デバイス向けの設定です。*	
	鍵:	• オプション 1 の全ての機能 • スロットは Lockable です。
	スロット:	• スロットが Writable である事を除き、オプション 1 と同じです。

表 3-19. スロット 13 の設定情報

スロット	設定値	有効機能
13	**オプション 1: Permanent Lock**	
	鍵:	**WPC スロット 0 デバイス圧縮証明書** • このスロットは、その他のデータの保存用として定義されます。
	スロット:	• データを上書きする事はできません。 • 平文でデータを読み出せます。
	オプション 2: Slot Lockable *Note:これはプロトタイプ デバイス向けの設定です。*	
	鍵:	• オプション 1 の全ての機能 • スロットは Lockable です。
	スロット:	• スロットが Writable である事を除き、オプション 1 と同じです。

表 3-20. スロット 14 の設定情報

スロット	設定値	有効機能
14	**オプション 1: Permanent Lock**	
	鍵:	**WPC スロット 0 MFG 圧縮証明書** • このスロットは、その他のデータの保存用として定義されます。
	スロット:	• データを上書きする事はできません。 • 平文でデータを読み出せます。
	オプション 2: Slot Lockable *Note:これはプロトタイプ デバイス向けの設定です。*	
	鍵:	• オプション 1 の全ての機能 • スロットは Lockable です。
	スロット:	• スロットが Writable である事を除き、オプション 1 と同じです。

表 3-21. スロット 15 の設定情報

スロット	設定値	有効機能
15	**オプション 1: Slot Lockable**	
	鍵:	**セキュアブート公開鍵** • このスロットは ECC 鍵向けに定義されます。 • スロットは Lockable です。
	スロット:	• ロックされていなければ、いつでも書き込み可能です。 • 常に読み出し可能です。
	オプション 2: Permanent Lock	
	鍵:	• スロットが恒久的にロックされる事を除き、オプション 1 と同じです。
	スロット:	• スロットが書き込めない事を除き、オプション 1 と同じです。

3.3 ECC608-TFLXWPC EEPROM OTP (One-Time-Programmable)ゾーン

OTP ゾーンは EEPROM アレイ内の 64 バイト(512 ビット) 領域であり、読み出し専用ストレージとして使います。このゾーンは、2 個のブロック(各 32 バイト)として構成されます。ECC608-TFLXWPC では、OTP ゾーンはロック済みで出荷され、以下の情報を格納します。

I²C デバイス バージョン

```
60   1B   1E   85   3B   13   C7   75   00   00   00   00   00   00   00   00
00   00   00   00   00   00   00   00   00   00   00   00   00   00   00   00
00   00   00   00   00   00   00   00   00   00   00   00   00   00   00   00
00   00   00   00   00   00   00   00   00   00   00   00   00   00   00   00
```

OTP ゾーンに書き込まれたデータバイト値は、4 バイトまたは 32 バイト読み出しを使っていつでも読み出せますが、変更はできません。

重要: OTP ゾーン内のバイトは今後変更される可能性があります。これらの値を暗号計算に使ってはいけません。

4. デバイスコマンド

以下では、ECC608- TFLXWPC で使用可能な全てのコマンドと、各コマンドのコマンドモードについて詳細に説明します。コマンドには以下の 3 つのカテゴリが存在します。

1. **一般デバイスコマンド**
   これらのコマンドは、さらに 2 つのカテゴリに分類されます。
   - **一般デバイス アクセスコマンド:** デバイスとのデータ送受信用に使います。通常、これらのコマンドは暗号機能を実行しません。
   - **一般暗号コマンド:** デバイスまたはシステムはこれらのコマンドを使えます。通常、これらのコマンドは特定データスロットを対象として実行されません。
2. **非対称暗号コマンド**
   これらのコマンドは、ECC 公開鍵または秘密鍵を使う非対称暗号演算(鍵の生成、メッセージの署名、メッセージの検証)を実行します。これらのコマンドは、ECC Data ゾーンスロットに対してのみ使用できます。
3. **対称暗号コマンド**
   これらのコマンドは対称暗号関数(ダイジェストまたは MAC の生成、鍵導出、AES 暗号化/復号等)を実行します。

全てのコマンドの入力パラメータ
特に明記しない限り、マルチバイトの入力パラメータは、入力パラメータ表にビッグエンディアン(MSB 先頭)として記載されます。ECC608-TFLXWPC は、データがリトルエンディアン(LSB 先頭)で送信される事を期待する事に注意が必要です。

表 4-1. コマンド オペコードの概要とコマンドカテゴリ

コマンド	概要	コマンドカテゴリ
Counter	モノトニック カウンタの 1 つを読み出すかインクリメントします。	一般デバイスコマンド
ECDH	保存されている秘密鍵と入力された公開鍵を使って ECDH プリマスタ秘密鍵を生成します。	非対称暗号コマンド
GenKey	ECC 公開鍵を生成します。オプションで ECC 秘密鍵を生成する事もできます。	非対称暗号コマンド
Info	デバイスのステート情報を返します。	一般デバイスコマンド
Lock	デバイスのゾーンまたはスロットに対する後続の変更を禁止します。	一般デバイスコマンド
Nonce	32 バイトの乱数と内部保存されるノンスを生成します。	一般デバイスコマンド
Random	乱数を生成します。	一般デバイスコマンド
Read	デバイスから 4 また 32 バイト(平文または暗号文)を読み出します。	一般デバイスコマンド
SecureBoot	電源投入時にコード署名またはコード ダイジェストを検証します。	非対称暗号コマンド
SelfTest	内部の各種暗号計算エレメントをテストするために使います。	一般デバイスコマンド
Sign	ECDSA 署名計算	非対称暗号コマンド
SHA	システムによって汎用的に使われる SHA-256 または HMAC ダイジェストを計算します。	一般デバイスコマンド
UpdateExtra	Configuration ゾーンがロックされた後に、Configuration ゾーン内のバイト 84 または 85 を更新するために使います。	一般デバイスコマンド

.....続き		
コマンド	**概要**	**コマンドカテゴリ**
Verify	ECDSA 検証計算	非対称暗号コマンド
Write	デバイスに 4 また 32 バイト(平文または暗号文)を書き込みます。	一般デバイスコマンド

4.1 一般デバイスコマンド

表 4-2 に、一般デバイスコマンドの一覧を示します。

表 4-2. 一般デバイスコマンド

コマンド名	概要
Counter	モノトニック カウンタのインクリメントと読み出しを行います。
Info	デバイスからリビジョンおよびステータス情報を読み出すために使います。
Lock	デバイス内のロック可能スロットを個々にロックするために使います。
Nonce	ノンス(1 度だけ使われる数)を生成するかデバイスに渡すために使います。
Random	システムによって使われる 32 バイト乱数を生成するために使います。
Read	デバイスの各種ゾーンを読み出すために使います。
SelfTest	内部の各種暗号計算エレメントをテストするために使います。
SHA	システムによって汎用的に使われる SHA-256 または HMAC ダイジェストを計算します。
UpdateExtra	Configuration ゾーンがロックされた後に、Configuration ゾーン内のバイト 84 または 85 を更新するために使います。
Write	デバイスに 4 また 32 バイトを書き込むために使います(平文または暗号文)。

4.1.1 Counter コマンド

Counter コマンドは、デバイスの Configuration ゾーン内に配置された 2 つのモノトニック カウンタの 1 つから 2 進数カウント値を読み出します。カウンタのカウント可能最大値は 2,097,151 です。この値を超えてカウントしようとすると、エラーコードが生成されます。これらのカウンタは、カウント動作中に給電が中断してもカウント値が失われないように設計されています。電源喪失条件によっては、カウント値が 2 つ以上インクリメントする場合があります。

ECC608-TFLXWPC の場合、カウンタはどの鍵にも割り当てられていませんが、システムによってカウンタを使う事ができます。各カウント値は既定値に設定され、最大値までカウント可能です。

4.1.2 Info コマンド

Info コマンドは、デバイスのステータスと状態を読み出すために使います。この情報は、エラーの特定と各種コマンドの実行に役立ちます。

4.1.3 Lock コマンド

ECC608-TFLXWPC の場合、Configuration ゾーンはロック済みであり、Data ゾーンのアクセスポリシーは設定済みです。しかし、一部のスロットは他のコマンドを使って更新可能です。必要に応じ、その中の一部のスロットは Lock コマンドの SlotLock モードを使って恒久的にロックできます。ロックすると、そのスロットは永久に変更できなくなります。

4.1.4 Nonce コマンド

Nonce コマンドは、乱数(内部または外部で生成可能)とシステムからの入力値を組み合わせる事により、後続のコマンド向けにノンス(Nonce: Number used Once)を生成します。

生成されたノンスは、内部で以下の 3 つのバッファのいずれかに保存されます。TempKey バッファ、メッセージダイジェスト バッファ、代替鍵バッファノンスを生成する代わりに固定値をデバイスに渡す事もできます。

4.1.5 Random コマンド

Random コマンドは、システムによって使われる乱数を生成します。乱数は内部の NIST 800-90 A/B/C 乱数生成器により生成されます。このコマンドは、常にバスへ 32 バイト値を出力します。この値をデータスロットまたは SRAM 内に保存する事はできません。

4.1.6 Read コマンド

Read コマンドを使うと、ECC608-TFLXWPC の全ての EEPROM ゾーンにアクセスできます。Data ゾーンへのアクセスは、スロットごとに設定されたアクセスポリシーにより制限されます。暗号読み出しは、特定のアクセスポリシーが設定された Data ゾーンスロットに対してのみ可能です。

4.1.7 SelfTest コマンド

SelfTest コマンドは、ECC608-TFLXWPC 内の 1 つまたは複数の暗号エンジンのテストを実行します。入力モードパラメータに応じて、全てまたは一部のアルゴリズムがテストされます。

ECC608-TFLXWPC の場合、電源投入または復帰イベント後の自動的な SelfTest コマンド実行は無効にされています。しかし、システムは必要に応じてこのコマンドを実行できます。このテストの実行に関する要件はありません。

電源投入または復帰時に自動的に実行された場合でも、このコマンドによって実行された場合でも、セルフテストに失敗するとデバイスは Failure ステートに移行し、デバイスの動作は制限されます。保存された Failure ステートは、復帰時または電源再投入時にクリアされます。

4.1.8 SHA コマンド

SHA コマンドは、システムによって汎用的に使われる SHA-256 または HMAC/SHA ダイジェストを計算します。SHA 計算は、ECC608-TFLXWPC の内部メモリの特別なセクション (コンテクスト バッファ)内で実行されます。他のコマンドを使ってこのセクションを読み書きする事はできません。SHA コマンドの各種フェイズとフェイズの間に任意のコマンドを挿入できます。その際の SHA コンテクストは、電源投入および復帰時に無効になります。SHA コマンドの実行中にエラーが発生しても、多くの場合はコンテクストが変更される事なく保持されます。

4.1.9 UpdateExtra コマンド

UpdateExtra コマンドは、UpdateExtra バイトと UpdateExtraAdd バイト(Configuration ゾーン内のバイト 84 とバイト 85)を更新するために使います。これらのバイトは、このコマンドによってのみ更新できます。これらのバイトは、現在の値が 0x00 である場合にのみ 1 度だけ更新が可能です。現在の値が 0x00 ではない場合、更新を試みるとエラーが発生します。

ECC608-TFLXWPC の場合、UpdateExtraAdd バイト (バイト 85) は代替 I^2C アドレスに設定されます。

4.1.10 Write コマンド

ECC608-TFLXWPC の場合、Configuration ゾーンと OTP ゾーンはロックされ、これらのゾーンの更新はできません。Data ゾーンに対する書き込みは、各スロットのアクセスポリシーに基づいて制限されます。書き込み可能なスロットについては、このコマンドの各モードの説明を参照してください。

4.2 非対称暗号コマンド

非対称暗号コマンドセットは、ECC 鍵を生成または使用するための特別なコマンドで構成されます。鍵は通常 Data ゾーンに保存されますが、一部のコマンドでは SRAM アレイに保存されます。

表 4-3. 非対称暗号コマンド

コマンド名	概要
ECDH	保存されている秘密鍵と入力された公開鍵を使って ECDH プリマスタ秘密鍵を生成します。
GenKey	保存されている秘密鍵から ECC 秘密鍵またはオプションにより ECC 公開鍵を生成します。
SecureBoot	電源投入時にコード署名またはコード ダイジェストを検証します。
Sign	ECC 秘密鍵を使って ECDSA 署名計算により内部または外部のメッセージ ダイジェストに署名します。
Verify	ECC 秘密鍵を使って ECDSA 検証計算により内部または外部のメッセージ ダイジェストを検証します。

4.2.1 ECDH コマンド

ECDH コマンドは、2 つのデバイスの間で共有する秘密鍵を生成します。2 つのデバイスは、それぞれ他方のデバイスから ECC 公開鍵を受け取り、スロットに保存されている ECC 秘密鍵または TempKey に保存されている使い捨て鍵と組み合わせます。これにより、両方のデバイスで同じ共有されたプリマスタ秘密鍵を生成します。さらに、この鍵を双方で共有する他のデータと組み合わせる事により、共有セッション鍵を生成する事ができます。共有秘密をさらに Diversify するため、KDF コマンドが TLS セッションでしばしば使われます。

4.2.2 GenKey コマンド

GenKey コマンドにより、ECC 秘密鍵の生成、秘密鍵からの ECC 公開鍵の生成、公開鍵ダイジェストの生成が可能です。このコマンドは、ECC 秘密鍵または公開鍵向けに設定されたスロットに対してのみ使えます。非 ECC スロットに対してこのコマンドを実行するとエラーが発生します。

4.2.3 SecureBoot コマンド

SecureBoot コマンドは、外部 MCU または MPU のセキュアブート向けのサポートを提供します。一般的に、システム内のブートコードは、ブート後に実行されるアプリケーション コードの検証を支援するために ECC608-TFLXWPC を使います。ECC608-TFLXWPC は、Stored Digest モードの SecureBoot コマンドを使って動作するよう設定されます。ダイジェストはスロット 7 に保存され、SecureBoot の検証に必要な公開鍵はスロット 15 に保存されます。オプションにより、持続性ラッチを使うよう設定できます。選択されたオプションに基づき、SecureBoot を電源投入に結び付けるかどうかが決まります。3.2.4 「セキュアブート オプション」を参照してください。

ホストと ECC608-TFLXWPC の間のケーブルでの改ざんを防ぐため、コマンドのモードに応じて、戻りコードの代わりに MAC を各種データ(TempKey に書き込まれたノンス、I/O 保護秘密鍵等)から生成できます。

4.2.4 Sign コマンド

Sign コマンドは、ECDSA アルゴリズムを使って署名を生成します。これには、KeyID によって指定されたスロット内の ECC 秘密鍵が使われます。何に署名するかに応じて異なるモードが利用できます。

4.2.5 Verify コマンド

Verify コマンドは、入力されたメッセージ ダイジェストと公開鍵に基づき、ECDSA [R,S]署名が正しく生成されたかどうかを検証します。いかなる場合も、署名がこのコマンドへの入力です。

中間者攻撃を防ぐため、Verify コマンドからオプションの MAC を返す事ができます。署名が入力ダイジェストから正しく生成された事が検証計算により示された場合、TempKey に保存されている入力ノンスと、ECC608-TFLXWPC とホスト MCU の両方に保存されている I/O 保護秘密鍵に基づいて、MAC が計算されます。MAC 出力は、External および Stored モードでのみ生成可能です。MAC を計算するには、I/O 保護機能を有効にする必要があります。

4.3 対称暗号コマンド

対称暗号コマンドセットは、対称鍵の生成または使用に関係するコマンドの集まりです。鍵は通常 Data ゾーンに保存されますが、一部のコマンドでは SRAM メモリアドレスに保存されます。

表 4-4. 対称暗号コマンド

コマンド名	概要
GenDig	乱数または入力シードと保存されている値からデータ ダイジェストを生成します。
MAC	SHA-256 を使って鍵とその他の内部データからダイジェスト (レスポンス)を計算します。

4.3.1 GenDig コマンド

GenDig コマンドは、SHA-256 ハッシュを使って、保存されている値または入力値と TempKey の内容を組み合わせます。このコマンドを実行する前に、TempKey の内容を検証する必要があります。保存値はデータスロットの 1 つ、Configuration ゾーン、いずれかの OTP ページ、モノトニック カウンタから取り込めます。デバイスのモードに応じて、GenDig 計算にどのデータを含めるかが決まります。

場合によっては、何らかのコマンドを実行する前に GenDig を実行する必要があります。与えられたコマンドを実行する前に、GenDig コマンドを複数回実行する事により、ダイジェストに追加のデータを含める事ができます。その結果得られたダイジェストは TempKye で保持され、以下の 4 通りの方法で使えます。

1. MAC、Sign、CheckMac コマンドによって使われるメッセージの一部としてダイジェストを含める事ができます。MAC レスポンス出力は GenDig 計算で使われたデータと MAC コマンドからの秘密鍵の両方を含むため、ダイジェストは Data および/または OTP ゾーンに保存されているデータの認証用に使えます。
2. 後続の Read または Write コマンドは、ダイジェストを使ってデータに認証および/または機密性を提供できます。この場合、ダイジェストはデータ保護ダイジェストと呼びます。
3. このコマンドは、トランスポート鍵配列からの値を使う事により、セキュア パーソナライズ用に使えます。結果として得られたデータ保護ダイジェストは、Write コマンドによって使われます。
4. 入力値(通常はリモートデバイスからのノンス)と現在の TempKey 値が組み合わされて共有ノンスが生成され、その中で両方のデバイスは RNG が含まれている事を証明できます。

4.3.2 MAC コマンド

MAC (Message Authentication Code) コマンドは、メッセージの SHA-256 ダイジェストを生成するために使われます。このダイジェストは、デバイス内に保存された鍵、チャレンジ、デバイスに関するその他の情報を含みます。このコマンドの出力は、このメッセージのダイジェストです。

このコマンドの通常の使用法は以下の通りです。

1. Nonce コマンドを実行して入力チャレンジをロードします。オプションにより、このチャレンジと生成された乱数を組み合わせる事ができます。この演算の結果は、ノンスとしてデバイス内部に保存されます。
2. 必要に応じ、GenDig コマンドを 1 回または複数回実行する事で、デバイス内の EEPROM 位置に保存されている値をノンスと組み合わせる事ができます。その結果はデバイス内部に保存されます。この機能により、複数の鍵をレスポンス生成の一部として使う事ができます。
3. この MAC コマンドを実行して上記ステップ 1 (および必要に応じてステップ 2) の出力と EEPROM 鍵を組み合わせる事で、出力レスポンス(すなわちダイジェスト)を生成します。

あるいは、同じ GenDig メカニズムを通して、秘密である事が要求されない任意のスロット内のデータをレスポンスに蓄積する事ができます。これは、その位置に保存されている値を認証する効果を有します。

5. I²C インターフェイス

I²C インターフェイスは、SDA ピンと SCL ピンを使って各種の I/O 状態を ECC608-TFLXWPC に対して示します。このインターフェイスは、1 MHz で動作する Microchip 社製 AT24C16 シリアル EEPROM とプロトコルレベルで互換となるよう設計されています。

Note: 2 つのデバイスは多くの点で異なります(例: ECC608-TFLXWPC と AT24C16 では既定値 I²C アドレスが異なります)。従って、各デバイスのデータシートを注意深く読む必要があります。

ECC608-TFLXWPC クライアントの出力ピンはオープンドレイン ドライバしか備えないため、SDA ピンは外付けプルアップ抵抗を使って High に駆動する必要があります。バスホストは、オープンドレインまたはトーテムポールが使えます。後者を使う場合、ECC608-TFLXWPC がバス上でデータを駆動している時にバスホストはトライステートになる必要があります。SCL ピンは入力であり、常に外部デバイスまたは外付け抵抗によって High および Low に駆動される必要があります。

注意: I²C 規格では「マスタ」および「スレーブ」という用語を使いますが、本書では同義の Microchip 社用語として「ホスト」および「クライアント」を使っています。

5.1 I/O 条件

本デバイスは以下の I/O 条件に応答します。

5.1.1 スリープ中のデバイス

スリープ中のデバイスは Wake 条件を除く全ての条件を無視します。

- Wake - SDA が t_{WLO} 以上の間 Low を保持した後に SDA の立ち上がりエッジが発生するとデバイスは低消費電力モードを終了します。遅延時間 t_{WHI} の後に、デバイスは I²C コマンドを受信可能となります。
- アイドルまたはスリープ中のデバイスは、t_{WLO} が過ぎるまで SCL ピン上の全てのレベルまたは状態遷移を無視します。t_{WHI} 中のある時点で SCL ピンが有効になり、デバイスは 5.1.2 「アクティブ中のデバイス」に記載した条件に応答します。

Wake 条件が成立するには、SDA ピンがシステム プロセッサによって t_{WLO} の間 Low に駆動されるか、0x00 のデータバイトが十分に遅い(すなわち SDA の Low 期間が t_{WLO} より長い)クロックレートで転送される必要があります。デバイスが復帰した時点で、通常のプロセッサ I²C ハードウェアおよび/またはソフトウェアはデバイス通信用に使用可能となります。デバイス通信には、デバイスを低消費電力(スリープ) モードへ戻すために必要な I/O シーケンスも含まれます。

ヒント: Wake パルスは、0x00 のバイトを 100 kHz で送信する事により簡単に生成できます。後続のコマンドは、これより高い周波数で実行できます。

I²C モードでは、既に復帰済みのデバイスは Wake シーケンスを無視します。

バス上に複数デバイスが存在する場合

バス上に複数のデバイスが存在する場合、I²C インターフェイスが約 300 kHz[1] 以下で動作すると、特定データパターンの送信によってバス上の ECC608-TFLXWPC が復帰します。周波数が低いほど、デバイスはより確実に復帰します。バスで送信される後続のデバイスアドレスは宛先のデバイスとのみ一致するため ECC608-TFLXWPC は応答しませんが、復帰はします。低周波数で他のデバイスと通信した後に、スリープまたはアイドル シーケンスを発行して ECC608-TFLXWPC を既知のステートに戻す事を推奨します。

[1] 実際の周波数は、デバイスごとの製造ばらつきと環境要因によって変化します。この値は、全ての条件でデバイスが確実に復帰できると見なせる周波数です。

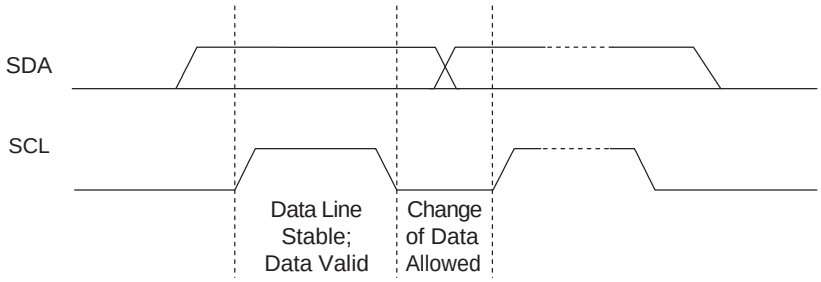
重要: t_{WLO} は、ECC608-TFLXWPC が全ての製造および環境条件で確実に復帰できるようにするためにシステムが提供する必要のある最小時間です。実際には、これよりも短いパルス幅でもデバイスは復帰します。

5.1.2 アクティブ中のデバイス

アクティブ中のデバイスは以下の条件に応答します。

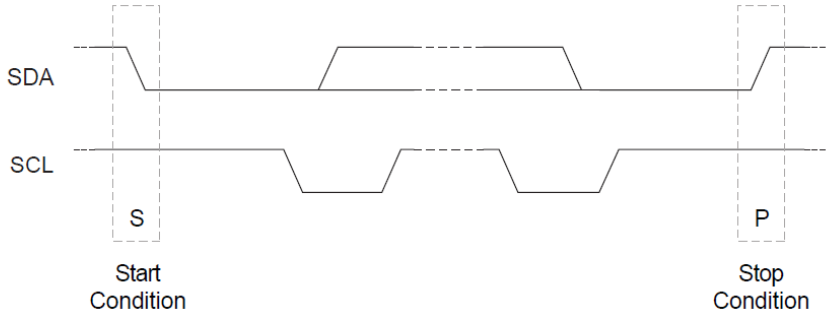
- **DATA = 0**: SCL が Low→High→Low と遷移する間 SDA が Low を保持した場合、「0」のビットがバス上で転送されます。SDA は SCL が Low の時に遷移できます。
- **DATA = 1**: SCL が Low→High→Low と遷移する間 SDA が High を保持した場合、「1」のビットがバス上で転送されます。SDA は SCL が Low の時に遷移できます。

図 5-1. I^2C インターフェイスにおけるデータビットの転送



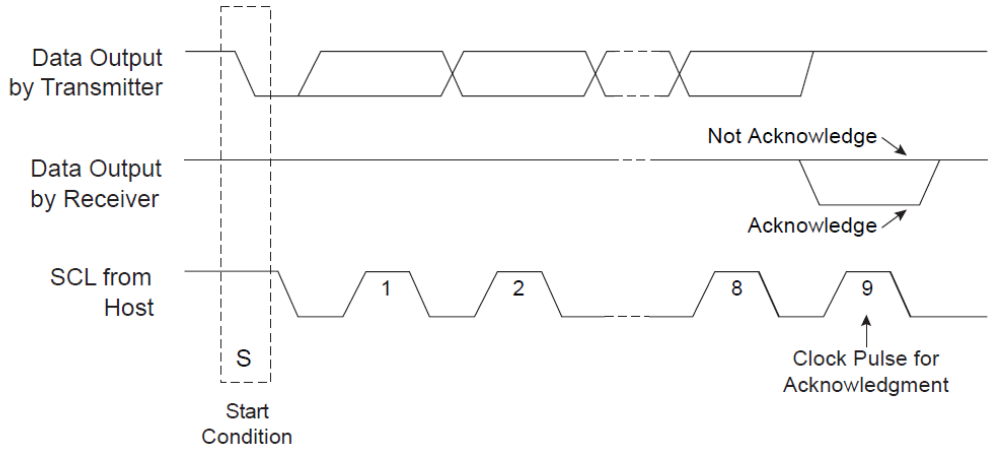
- **スタート条件**: SCL が High の時に SDA が High から Low へ遷移するとスタート条件が発生します。全てのコマンドの前にスタート条件が必要です。
- **ストップ条件**: SCL が High の時に SDA が Low から High へ遷移するとストップ条件が発生します。デバイスは、ストップ条件を受信した後に現在の I/O トランザクションを終了します。デバイスはコマンドの実行に必要な全てのバイトを入力で受信すると、ビジー状態に移行してコマンドの実行を開始します。ストップ条件は、デバイスへ送信される全てのパケットの最後で送信される必要があります。

図 5-2. I^2C インターフェイスのスタート条件とストップ条件



- **Acknowledge (ACK)**: 各アドレスバイトまたはデータバイトが転送された後の 9 番目のクロックサイクルで、レシーバは SDA ピンを Low にする事によって、そのバイトを正常に受信した事を知らせます。
- **否定応答(NACK)**: 各アドレスバイトまたはデータバイトが転送された後の 9 番目のクロックサイクルで、レシーバは SDA ピンを High のままにする事によって、そのバイトの受信に問題があった事またはそのバイトでそのグループの転送が完了する事を知らせます。

図 5-3. I²C インターフェイスの NACK および ACK 条件



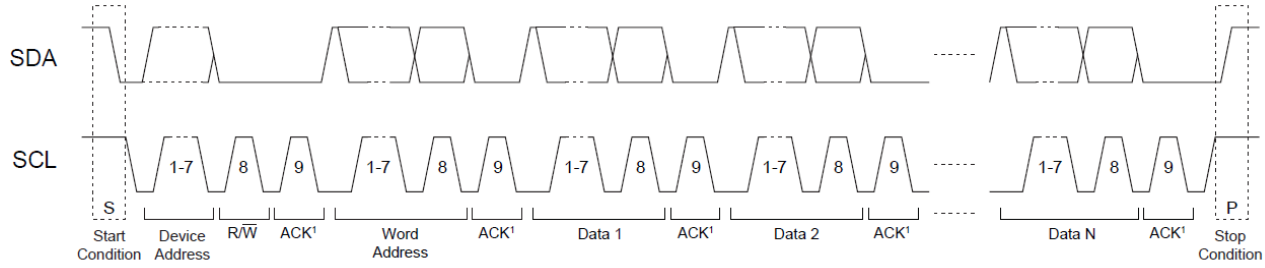
Configuration ゾーン内で設定されている I2C_Address が互いに異なる複数の ECC608-TFLXWPC は、同じ I²C インターフェイス信号を容易に共有できます。デバイスアドレスの 7 ビットは全て設定可能であるため、ECC608-TFLXWPC はシリアル EEPROM を含む任意の I²C デバイスとの間で I²C インターフェイスを共有する事もできます。

5.2 ECC608-TFLXWPC への I²C 送信

システムから ECC608-TFLXWPC へのデータ送信の概要を図 5-4 に示します。送信の順序は以下の通りです。

- スタート条件
- デバイスアドレス バイト
- ワードアドレス バイト
- データバイト(1～N) (必要に応じて)
- ストップ条件

図 5-4. ECC608-TFLXWPC への標準的な I²C 送信



ACK 期間中に SDA は ECC608-TFLXWPC によって Low に駆動されます。

表 5-1 に、I/O トランザクションの各バイトを示します。「I²C 名」列は、AT24C16 のデータシートに記載されているバイト名です。

表 5-1. ECC608-TFLXWPC への I²C 送信

名称	I²C 名	概要
Device Address	Device Address	このバイトは、I2C インターフェイス上で特定デバイスを選択します。このバイトの bit 1～7 が Configuration ゾーン内の I2C_Address バイトの bit 1～7 に一致すると、その ECC608-TFLXWPC が選択されます。このバイトの bit 0 は標準 I2C の R/W ビットであり、書き込み動作(デバイスアドレス バイトに続くバイトをホストからクライアントへ転送する)を示す「0」である事が必要です。
Word Address	Word Address	通常動作では、このバイトの値は 0x03 である事が必要です。

.....続き		
名称	I²C 名	概要
Command	Data1, N	カウント、コマンドパケット、2 バイト CRC で構成されるコマンドグループです。CRC は、サイズおよびパケットバイトに対して計算されます。

本デバイスはコマンド入力バッファを FIFO として扱うため、入力グループは 1 つまたは複数の I²C コマンドグループに格納してデバイスへ送信できます。デバイスへ最初に送信されるバイトはカウント(この後にデバイスが受信するバイトの数)です。デバイスは、実行が終了するまでこの数を超える後続の受信バイトを無視します。

システムは、最後のコマンドバイトの後にストップ条件を送信する必要があります。これにより、ECC608-TFLXWPC はコマンドの処理を開始します。ストップ条件を送信しないと、最終的に同期が喪失する可能性があります。
リカバリ手順は 5.2.2 「同期」を参照してください。

関連リンク

5.2.1 ワードアドレス バイト

5.2.1 ワードアドレス値

I²C パケット書き込み中は、ECC608-TFLXWPC は 2 番目のバイトをワードアドレスとして解釈します。ワードアドレス値は、表 5-2 の通りにパケットの機能を示します。

表 5-2. ワードアドレス値

名称	値	概要
Reset	0x00	アドレスカウンタをリセットします。次の読み出しまたは書き込みトランザクションは、I/O バッファの先頭位置で始まります。
Sleep (Low-power)	0x01	ECC608-TFLXWPC は低消費電力スリープモードに移行し、次の Wake フラグまで後続の I/O トランザクションを全て無視します。デバイスの揮発性ステートは全てリセットされます。
Idle	0x02	ECC608-TFLXWPC はアイドルモードに移行し、次の Wake フラグまで後続の I/O トランザクションを全て無視します。TempKey、メッセージ ダイジェスト バッファ、代替鍵レジスタの内容は保持されます。
Command	0x03	後続のバイトを入力コマンドバッファ(前回の書き込み位置の次のアドレス)に書き込みます。これは標準の動作です。
予約済み	0x04 – 0xFF	これらアドレス値をデバイスへ送信してはいけません。

5.2.2 I²C の同期

システムリセットや I/O ノイズ等によってシステムと ECC608-TFLXWPC 上の I/O ポートの間の同期が失われる可能性があります。このような場合、ECC608-TFLXWPC は期待通りに応答できなくなります(スリープ状態になるか、システムがデータを送信しようとしているタイミングでデータを送信してしまう等)。再同期するには、以下の手順が必要です。

1. I/O チャンネルを確実にリセットするため、システムは以下の通りに標準 I²C ソフトウェア リセット シーケンスを送信する必要があります。
   - スタートビット条件
   - システムのプルアップ抵抗によって SDA を High に保持した状態で 9 サイクルの SCL
   - 次のスタートビット条件
   - ストップビット条件

   以上の手順によって同期が正しく確立されると、読み出しシーケンスの送信が可能になり、ECC608- TFLXWPC はデバイスアドレスに対して ACK を返します。データ期間中に、デバイスはデータを返すかバスをフロート状態(システムによって値が 0xFF のデータとして解釈される) にします。

   デバイスがデバイスアドレスに対して ACK を返した場合、システムは内部アドレスカウンタをリセットする必要があります。これにより、ECC608- TFLXWPC はそれまでに送信された不完全な入力コマンドを無視します。アドレスカウンタは、ワードアドレス 0x00 (リセット)への書き込みシーケンスを送信した後にストップ条件を生成する事によりリセットできます。

2. デバイスがデバイスアドレスに対して ACK で応答しない場合、デバイスはスリープ中である可能性があります。この場合、システムは完全な Wake トークンを送信し、立ち上がりエッジ後に t_{WHI} が過ぎるまで待機する必要があります。その後、システムは読み出しシーケンスを再度送信できます。同期が確立されていれば、デバイスはデバイスアドレスに対して ACK を返します。
3. それでもデバイスがデバイスアドレスに対して ACK で応答しない場合、デバイスはビジー状態(コマンドの実行中)である可能性があります。
   システムは最長の t_{EXEC}(max)が過ぎるまで待機してから読み出しシーケンスを送信する事で、デバイスから ACK が返されます。

5.3 スリープ シーケンス

システムが ECC608-TFLXWPC の使用を終了した時点で、システムからスリープ シーケンスを発行してデバイスを低消費電力モードに移行させる事を推奨します。このシーケンスはデバイスアドレス、値 0x01 (ワードアドレス)、ストップ条件で構成されます。低消費電力状態に移行すると、デバイスの内部コマンドエンジンと入出力バッファは完全にリセットされます。このシーケンスは、デバイスがアクティブかつ非ビジーの時にいつでもデバイスへ送信できます。

5.4 アイドル シーケンス

コマンドの総シーケンス時間が $t_{WATCHDOG}$ を超えた場合、デバイスは自動的にスリープに移行し、揮発性レジスタ内の情報は全て失われます。これを防ぐには、ウォッチドッグ期間が終了する前にデバイスをアイドルモードに移行させる必要があります。デバイスは、Wake トークンを受信した時にウォッチドック タイマを再始動し、実行を継続できます。

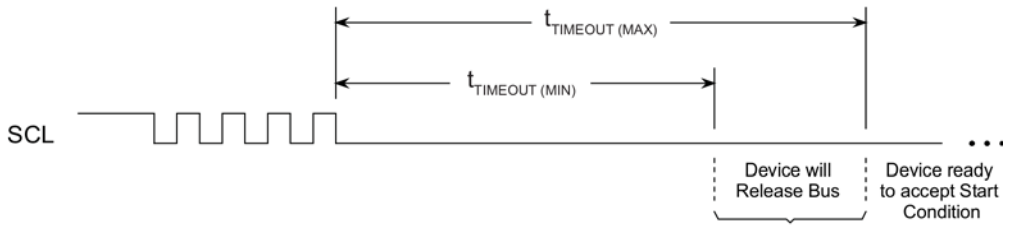
このアイドル シーケンスはデバイスアドレス、値 0x02 (ワードアドレス)、ストップ条件で構成されます。このシーケンスは、デバイスがアクティブかつ非ビジーの時にいつでもデバイスへ送信できます。

5.5 SMBus タイムアウト

ECC608-TFLXWPC は SMBus タイムアウト機能をサポートします。この機能により、SCL ピンが最小 $t_{TIMEOUT}$ 仕様値より長く Low を保持した場合に、ECC608-TFLXWPC はそのシリアル インターフェイスをリセットして SMBus を開放します(バスの駆動を停止して SDA をフロート High 状態にします)。

最小 $t_{TIMEOUT}$ に達した時点で、デバイスはスリープモードに移行します。最大 $t_{TIMEOUT}$ が経過した後に、ECC608-TFLXWPC は新しい復帰シーケンスとこれに続くスタート条件を受け入れ可能となります。

図 5-5. SMBus タイムアウト



5.6 ECC608-TFLXWPC からの I²C 送信

ECC608-TFLXWPC がアクティブであり、かつビジー状態ではない場合、ホストは I^2C 読み出しを使ってデバイスから現在の出力バッファの内容を読み出せます。有効なコマンド結果が得られた場合、返されるグループのサイズは、実行されるコマンドによって決まります。結果が無効である場合、グループ(および返される最初のバイト)のサイズは常に 4 (カウントバイト + ステータス/エラー バイト + 2 バイトの CRC)です。

表 5-3. ECC608-TFLXWPC からの I²C 送信

名称	I²C 名	方向	概要
Device Address	Device Address	To Client	このバイトは I²C インターフェイス上の特定デバイスを選択します。このバイトの bit 1～7 が Configuration ゾーン内の I2C_Address バイトの bit 1～7 に一致すると、その ECC608-TFLXWPC が選択されます。このバイトの bit 0 は標準 I2C の R/W ビットであり、読み出し動作(デバイスアドレス バイトに続くバイトをクライアントからホストへ転送する)を示す「1」である事が必要です。
Data	Data1, N	To Host	出力グループはカウントバイト + ステータス/エラーバイトまたは出力パケット + 2 バイトの CRC で構成されます。

ホストはステータス、エラー、コマンド出力を繰り返し読み出せます。I²C インターフェイスを介して ECC608-TFLXWPC へ Read コマンドが送信されるたびに、デバイスは出力バッファ内の次のバイトを送信します。本デバイスによるアドレスカウンタの扱い方は、この後で説明します。

ECC608-TFLXWPC がビジー、アイドル、スリープ状態のいずれかである場合、デバイスは読み出しシーケンス中のデバイスアドレスに対して NACK を返します。部分的なコマンドがデバイスへ送信された後に読み出しシーケンス[Start + DeviceAddress(R/W == R)] がデバイスへ送信された場合、ECC608-TFLXWPC はデバイスアドレスに対して NACK を返す事で、読み出し可能なデータが存在しない事を示します。

関連リンク

7.3.1 「AC パラメータ: I2C インターフェイス」

6. 応用のための情報

ECC608-TFLXWPC は、Microchip 社の Trust CryptoAuthentication™ファミリに属します。TrustFLEX ファミリの製品は使いやすくて簡単に実装でき、セキュアなプロビジョニングのために Microchip 社の技術とインフラストラクチャを活用できます。また、たとえ小量生産であってもエンドシステムにセキュリティ機能を実装する事ができます。

ATECC608B-TFLXTLS は、Qi ワイヤレス充電トランスミッタにセキュリティ機能を追加する際の煩雑な手間を省く事を目的に開発されました。本デバイスは、1 つまたは 2 つの WSP 証明書スロットチェーンを保存するよう設定済みです。WPC スロット 1 証明書チェーンが使われない場合、独自の証明書チェーンを保存して WPC スロット 2 と関連付ける事ができます。

加えて、ECC608-TFLXWPC は、ATECC608B-TFLXTLS および ATECC608B-TNGTLS 製品と同様のシームレスな方法で IoT クラウドへの接続をサポートします。これにより、産業用インフラストラクチャ (レストラン、ホテル等)のアプリケーションで使われるワイヤレス充電向けの接続が可能です。これらの接続が必要である場合、本デバイス内のセキュアブート機能を使って、クラウドへの接続前にワイヤレス充電トランスミッタ内のマイクロコントローラのファームウェアを確認する事もできます。

Microchip 社は、セキュリティ デバイスに加えて各種ツールも開発しています。これらのツールにより、弊社のハードウェア デバイスをシームレスに統合し、セキュリティ ソリューション全体を容易に開発できます。Microchip 社のソフトウェア セキュリティ ツールを使う事で、インフラストラクチャのセットアップが容易にでき、初期プロトタイプから製造まで開発を迅速に進める事ができます。

6.1 WPC 規約

Qi 認証製品を販売する全ての企業は、WPC のメンバーである事が必要です。Qi 認証製品として販売される全ての製品は、Qi 規格が指定する検証、試験、認証手順を通過する必要があります。これらの手順を通過しない限り、製品を Qi 準拠または Qi 認証済みと主張する事は許されません。Qi 認証製品の製造者は、WPC の規約に従う必要があります。

認証が必要な Qi 1.3 準拠製品の場合、追加の規約が要求されます。認証を必要とする製品を製造するには、Qi 認証済み製造者として認可される必要があります。認証が必要な製品は、ECC P-256 秘密鍵を安全に保存するためのセキュア ストレージ サブシステム(SSS)を備える必要があります。SSS を提供する企業は、認可された WPC Qi 製造 CA である事が必要です。Microchip 者は、SSS の要件を満たす各種製品を提供しており、ECC608-TFLXWPC はその中の 1 つです。Microchip 社は認可された Qi 製造 CA です。

Qi 製品の製造者には Qi 認証済みプロバイダから SSS を選定する責任があり、製造 CA にはその製造者が WPC の規約に従っている事を確認する責任があります。

セキュア ブートローダのプロビジョニング フロー

WPC 量産ユニットの標準的なプロビジョニング フローは以下の通りです。

1. お客様が ECC608-TFLXWPC を使った製品の開発を始めます。
2. お客様は、プロビジョニング済み SSS 向けの Microchip Sales Force サポートケースを作成します。
3. お客様は、サポートチケット システムを通して PTMC と Qi ID を Microchip 社に提供します。
4. それらの情報に基づき、Microchip 社は WPC と一緒にお客様のオーナーシップを確認します。
5. 確認が取れた後、Microchip 社は適切な証明書を生成し、製造証明書に対する証明書署名要求を WPC ルート CA と一緒にセットアップします。(Note:これが発生した時、WPC と一緒にチェックします)
6. 署名手続きが完了した後に、Microchip 社は限られた数の検証用デバイスをお客様に提供します。お客様は、それらのデバイスが正しくプログラミングされ、お客様の要求を全て満たしているか評価します。
7. お客様は、検証用デバイスを承認する事を Microchip 社に通知します。
8. お客様は、WPC 認証試験を進めます。
9. 認証試験が正常に完了した後に、お客様は必要数の量産用デバイスを要求できます。

6.2 ユースケース

ECC608-TFLXWPC は、WPC Qi 充電器の認証要求向けに専用設計されています。Microchip 社は、WPC の認可を受けた製造 CA です。セキュリティ IC に加えて、Microchip 社はワイヤレス充電向けの完全なパワーレシーバおよびパワー トランスミッタ ソリューション(認証あり/なし)も提供しています。

セキュア TLS 接続
ECC608-TFLXWPC は、各種のプロトコルを使ったセキュア TLS 接続をサポートします。このアプリケーションは WPC 認証要件の範囲外ですが、Qi インフラストラクチャ市場における Qi トランスミッタの急速な普及を可能にする重要な要因であると考えられています。

セキュアブート
マイクロコントローラまたはマイクロプロセッサのブートイメージの保護は、多くのベンダーにとっての懸念事項です。実行中のコードが信頼できる事(改ざんされていない事)を検証するための機能により、システム全体の保全性が維持されます。ECC608-TFLXWPC は、システムのコード ダイジェストをデバイスのデータスロットに保存する事によりセキュアブートを可能にするよう設定されています。コードの初期実行時に、システムはシステム ファームウェアに対するダイジェストを再構成し、それを ECC608-TFLXWPC に保存されているダイジェストと比較する事で、ファームウェアが改ざんされていない事を確認できます。加えて、デバイスの設定に基づき、セキュアブートが発生するまで TLS または WPC トランスミッタの認証を抑止する事ができます。

一般的データストレージ
システムに小量の追加情報を保存したい場合があります。ECC608- TFLXWPC では、データの読み書きが可能なデータスロットを使う事により、EEPROM メモリデバイスを追加しなくてもそれらの情報を保存できます。このため、データを保存するためだけに EEPROM メモリデバイスを追加する必要はありません。

6.3 開発ツール

ECC608- TFLXWPC は各種のハードウェアおよびソフトウェア ツールと、アプリケーション開発を迅速に進めるためのバックエンド サービスによりサポートされます。初期開発は、使いやすい Trust Platform Design Suite ツール ファミリを使って始める事ができます。これらのツールは、ユースケースを実装するためのグラフィカルな手段を提供し、最終的にアプリケーションの実装に必要な C コードを生成します。

定義済みの Trust Platform Design Suite ツールがお客様のアプリケーションに対応していない場合、CryptoAuthLib または CryptoAuthLib の Python® バージョンと CryptoAuthTool を使ってアプリケーションを開発できます。CryptoAuthLib は、Trust Platform Design Suite ツールから出力されるコードのバックボーンでもあります。

ハードウェア ツールと ECC608- TFLXWPC のサンプルデバイスにより、アプリケーションの完全な検証が可能です。本デバイスのアクセスポリシーは設定済みであるため、お客様はシステムレベルのコード開発に集中できます。

アプリケーションが完成したら、Microchip 社から ECC608- TFLXWPC デバイスを注文できます。

6.3.1 Trust Platform Design Suite

実装手順を簡素化するため、Microchip 社はウェブベースの Trust Platform Design Suite ツールを開発しました。これらのツールは、コンセプト段階から量産段階までお客様の開発を支援します。これらのツールを使うと、ECC608- TFLXWPC のコンフィグレーションと定義済みアクセスポリシーによる制約内で、特定のアプリケーションを実装するために必要なトランザクション ダイアグラムとコードを開発できます。

Note: これらのツールの詳細は、Microchip 社ウェブサイトの Trust Platform 製品ページご覧になれます。

6.3.2 ハードウェア ツール

ECC608-TFLXWPC を使ったアプリケーションの開発には、各種のハードウェア ツールが役立ちます。本書に記載していないツールについては、Microchip 社ウェブサイトをご覧ください。各ツールの説明には、ユースケースの例も記載しています。

DM320118 - CryptoAuthentication Trust プラットフォーム

DM320118 は ATSAMD21 マイクロコントローラ、ATECC608B-TNGTLS/ATECC608B-TFLXTLS/ATECC608B-TCSTM Trust デバイス(各 1 個ずつ)、USB ハブ、mikroBUS コネクタ、オンボード デバッガを備えたコンパクトな開発システムです。Trust Platform Design Suite ツールを使って Trust デバイスによる各種ユースケースを実装できます。このキットを MPLAB® X または Microchip Studio Design 環境で使う事により、その他のアプリケーションも開発できます。mikroBUS アドオンボードにより、ECC608-TFLXWPC をこのキットで使う事ができます。

DM320109 - CryptoAuthentication スタータキット

DM320109 は ATSAMD21-XPRO 開発ボードにより構成され、CryptoAuthentication デバイスで動作するファームウェアがプログラミング済みです。このキットには AT88CKSCKTSOIC-XPRO ソケットボードが同梱されますが、サンプルデバイスは UDFN パッケージでのみ提供されるため、UDFN バージョンのボードが別途必要です。ECC608-TFLXWPC のサンプルデバイスを別途入手する必要があります。

AT88CKSCKTUDFN(SOIC)-XPRO

AT88CKSCKTUDFN-XPRO と AT88CKSCKTSOIC-XPRO は、XPRO インターフェイスを備えた任意のマイクロコントローラ開発ボードと一緒に使える汎用的な CryptoAuthentication ソケットキットです。ECC608- TFLXWPC のサンプルデバイスを別途入手する必要があります。

Microchip ワイヤレスパワー ソリューション

Microchip 社は、dsPIC®デジタルシグナル コントローラに基づく完全なワイヤレス パワー トランスミッタおよびレシーバ ソリューションも提供しています。これらのソリューションは Qi 1.3 (認証を要求)と Qi 1.2 の両方に対応する他、その他の独自ソリューションにも対応可能です。Microchip 社のワイヤレス ソリューションの詳細は www.microchip.com/en-us/solutions/power-management-and-conversion/intelligent-power/wireless-power でご覧ください。

6.3.3 CryptoAuthLib

CryptoAuthLib は、Microchip 社の CryptoAuthentication デバイスファミリをサポートするソフトウェア ライブラリです。ECC608-TFLXWPC を使ったアプリケーションの開発には、このライブラリを使用する事を推奨します。このライブラリは、本書に記載したコマンドを実行するために必要な API 関数の呼び出しを実装します。

このライブラリは、多くの Microchip 社製マイクロコントローラで簡単に動作させる事ができますが、HAL (Hardware Abstraction Layer)を介して他のマイクロコントローラ(他社製品を含む)向けに容易に拡張できます。

これらのツールの詳細は、以下でご覧ください。

- CryptoAuthLib – Web Link
- CryptoAuthLib – GitHub

API 関数の呼び出し

本書に記載した各コマンドには、1 つまたは複数の API 呼び出しが割り当てられています。通常、全ての入力パラメータを指定可能なベース AP 呼び出しが存在します。コマンドおよびサブセクションに示されるパラメータは、このコマンドで使えます。各 API 呼び出しには複数のモードがあります。下表にコマンドとベース API 呼び出しの例を示します。詳細な API 情報は、GitHub 情報を参照してください。

表 6-1. CryptoAuthLib API 関数の呼び出しに対するコマンド例

デバイスコマンド	API 呼び出し	注釈
Info	atcab_info_base()	
Write	atcab_write()	
Read	atcab_read_zone()	
SHA	atcab_sha_base()	
Sign	atcab_sign_base()	
Random	atcab_random()	

.....続き

デバイスコマンド	API 呼び出し	注釈
Verify	atcab_verify()	

7. 電気的特性

7.1 絶対最大定格

動作温度	-40～+85 ℃
保管温度	-65～+150 ℃
最大動作電圧	6.0 V
DC 出力電流	5.0 mA
全ピンの電圧 -0.5 V～(V_{CC} + 0.5 V)	-0.5 V～(V_{CC} + 0.5 V)
ESD 耐圧:	
HBM	4 kV 以上
CDM	1 kV 以上

Note: ここに記載した「絶対最大定格」を超える条件は、デバイスに恒久的な損傷を生じさせる可能性があります。これはストレス定格です。本書の動作表に示す条件外でのデバイスの運用は想定していません。絶対最大定格条件を超えて長期間暴露させるとデバイスの信頼性に影響が及ぶ可能性があります。

7.2 信頼性

ECC608-TFLXWPC は Microchip 社の高信頼性 CMOS EEPROM 製造技術を採用しています。

表 7-1. EEPROM の信頼性

パラメータ	Min.	Typ.	Max.	単位
書き込み耐性 @+85 ℃(各バイト)	400,000	–	–	書き込みサイクル
データ保持寿命 @+55 ℃	10	–	–	年
データ保持寿命 @+35°C	30	50	–	年
読み出し耐性	制限なし			読み出しサイクル

7.3 AC パラメータ:全 I/O インターフェイス

図 7-1. AC タイミング図: 全インターフェイス

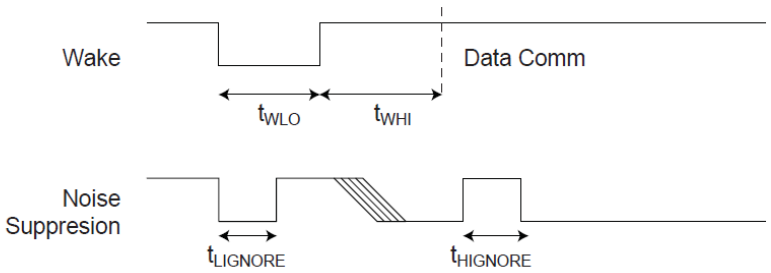


表 7-2. AC パラメータ: 全 I/O インターフェイス

パラメータ	シンボル	方向	Min.	Typ.	Max	単位	条件
電源投入遅延 [2]	t_{PU}	To Crypto Device	100	–	–	µs	V_{CC} > V_{CC}min から t_{WLO} の開始までの最小時間
復帰 Low 期間	t_{WLO}	To Crypto Device	60	–	–	µs	–
データ通信開始前の復帰 HIGH 遅延	t_{WHI}	To Crypto Device	1500	–	–	µs	ポーリング方式を採用していない場合、この期間中に SDA が安定して High を保持する事を推奨します。電源投入時にセルフテスト機能は無効です。
セルフテスト機能が有効な場合の復帰 HIGH 遅延	t_{WHIST}	To Crypto Device	20	–	–	ms	ポーリング方式を採用していない場合、この期間中に SDA が安定して High を保持する事を推奨します。
アクティブ時 High レベル グリッチ フィルタ	$t_{HIGNORE\_A}$	To Crypto Device	45[1]	–	–	ns	アクティブ時に、デバイスはそのステートに関係なく、この時間より短いパルスを無視します。
アクティブ時 Low レベル グリッチ フィルタ	$t_{LIGNORE\_A}$	To Crypto Device	45[1]	–	–	ns	アクティブ時に、デバイスはそのステートに関係なく、この時間より短いパルスを無視します。
スリープ時 Low レベル グリッチ フィルタ	$t_{LIGNORE\_S}$	To Crypto Device	15[1]	–	–	µs	スリープモード時に、デバイスはこの時間より短いパルスを無視します。
ウォッチドッグ タイムアウト	$t_{WATCHDOG}$	To Crypto Device	0.7	1.3	1.7	s	Config.ChipMode[2] = 0 の場合、復帰してからデバイスをスリープモードへ移行させるまでの時間です。

Note:

1. これらのパラメータは特性データであり、製造時の検査は実施していません。
2. Configuration ゾーン内で電源投入時セルフテスト機能が有効にされている場合、電源投入遅延時間は大幅に増加します。

7.3.1 AC パラメータ:I²C インターフェイス

図 7-2. I²C 同期データのタイミング

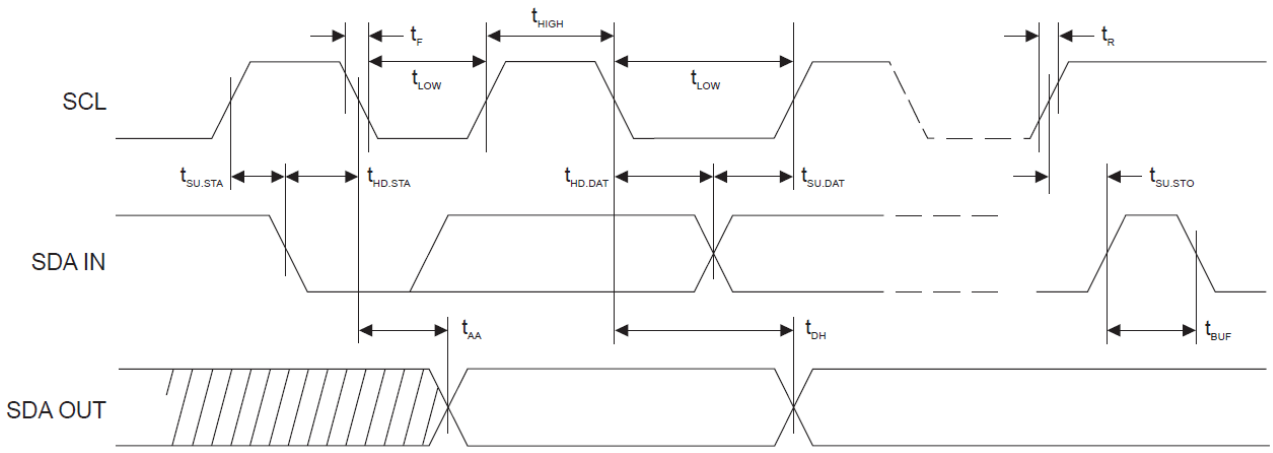


表 7-3. I²C インターフェイスの AC 特性(2)

特に明記しない限り、T_A = -40～+ +85°C、V_{CC} = +2.0～+5.5 V、C_L = 1 TTL ゲート+100 pF の推奨動作レンジに適用

パラメータ	シンボル	Min.	Max.	単位
SCL クロック周波数	f_{SCL}	0	1	MHz
SCL High 時間	t_{HIGH}	400	–	ns
SCL Low 時間	t_{LOW}	400	–	ns
スタート条件セットアップ時間	$t_{SU.STA}$	250	–	ns
スタート条件ホールド時間	$t_{HD.STA}$	250	–	ns
ストップ条件セットアップ時間	$t_{SU.STO}$	250	–	ns
データ入力セットアップ時間	$t_{SU.DAT}$	100	–	ns
データ入力ホールド時間	$t_{HD.DAT}$	0	–	ns
入力立ち上がり時間 [1]	tR	–	300	ns
入力立ち下がり時間 [1]	tF	–	100	ns
クロック Low からデータ出力確定までの時間	t_{AA}	50	550	ns
データ出力ホールド時間	t_{DH}	50	–	ns
SMBus タイムアウト遅延	$t_{TIMEOUT}$	25	35	ms
次の伝送が開始可能になるまでに必要なバスフリー時間 [1]	t_{BUF}	500	–	ns

Note:

1. これらのパラメータは特性データであり、製造時の検査は実施していません。
2. AC 計測条件:
   - R_L (SDA と V_{CC} の間を接続): 1.2 kΩ (V_{CC} = +2.0～+5.0 V)
   - 入力パルス電圧: $0.3V_{CC}$ ～$0.7V_{CC}$
   - 入力立ち上がり/立ち下がり時間: ≤ 50 ns
   - 入出力タイミング参照電圧: $0.5V_{CC}$

7.4 DC パラメータ:全 I/O インターフェイス

表 7-4. 全 I/O インターフェイスの DC パラメータ

パラメータ	シンボル	Min.	Typ.	Max.	単位	条件
動作時周囲温度	T_A	-40	–	+85	℃	標準産業用温度レンジ
電源電圧	V_{CC}	2.0	–	5.5	V	–
アクティブ時消費電流	I_{CC}	–	2	3	mA	I/O 転送中の I/O 待機時または非 ECC コマンドの実行時(クロック分周値とは無関係)
		–	–	14	mA	ECC コマンドの実行時(クロック分周比 = 0x0)
アイドル時消費電流	I_{IDLE}	–	800	–	µA	デバイスがアイドルモード中の時、 V_{SDA} および V_{SCL} < 0.4 V または > V_{CC} – 0.4 V
スリープ電流	I_{SLEEP}	–	30	150	nA	デバイスがスリープモード中の時、V_{CC} ≤ 3.6 V、 V_{SDA} および V_{SCL} < 0.4 V または > V_{CC} – 0.4 V、 TA ≤ +55 ℃
		–	–	2	µA	デバイスがスリープモード中の時 V_{CC} および温度の全レンジに適用

.....続き

パラメータ	シンボル	Min.	Typ.	Max.	単位	条件
出力 Low 電圧	V_{OL}	–	–	0.4	V	デバイスがアクティブモード中の時、 V_{CC} = 2.5～5.5 V
出力 Low 電流	I_{OL}	–	–	4	mA	デバイスがアクティブモード中の時、 V_{CC} = 2.5～5.5 V、V_{OL} = 0.4 V
接合部-大気間熱抵抗	Θ_{JA}	–	166	–	℃/W	SOIC (SSH)
		–	173	–	℃/W	UDFN (MAH)

7.4.1 V_{IH} と V_{IL} の仕様

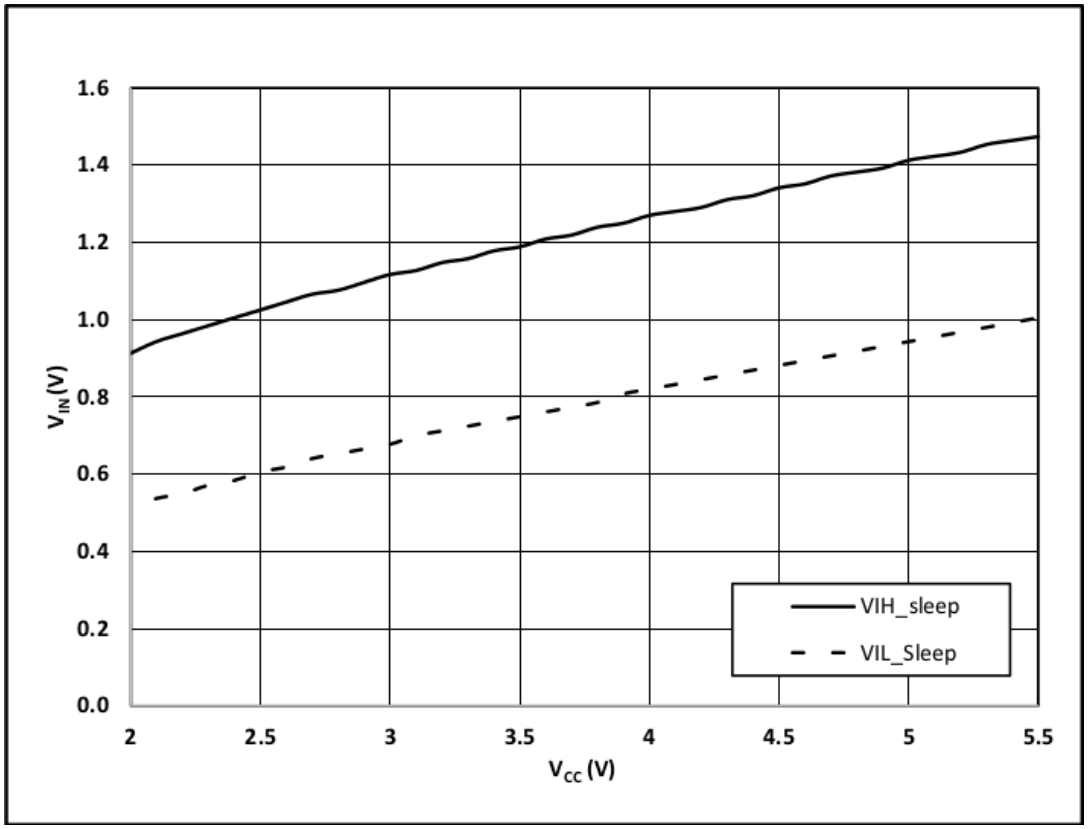
デバイスの入力レベルは、デバイスのモードと電圧に応じて変化します。スリープまたはアイドルモード中の入力電圧しきい値は、図 7-3 に示す通り、V_{CC} レベルに応じて変化します。スリープまたはアイドルモード中は、TTLenable ビットは効力を有しません。

ECC608-TFLXWPC のアクティブ入力レベルは固定されており、V_{CC} レベルと一緒に変化しません。デバイスへ送信される入力レベルは、下表に従う必要があります。

表 7-5. 全 I/O インターフェイスでの V_{IL} と V_{IH} (TTLenable = 0)

パラメータ	シンボル	Min.	Typ.	Max.	単位	条件
入力 Low 電圧	V_{IL}	-0.5	–	0.5	V	デバイスがアクティブかつコンフィグレーション メモリ内の TTLenable ビットが「0」の場合 (これ以外の場合は上記参照)
入力 High 電圧	V_{IH}	1.5	–	V_{CC} + 0.5	V	デバイスがアクティブかつコンフィグレーション メモリ内の TTLenable ビットが「0」の場合 (これ以外の場合は上記参照)

図 7-3. スリープおよびアイドルモード中の V_{IH} と V_{IL}



8. パッケージ図面

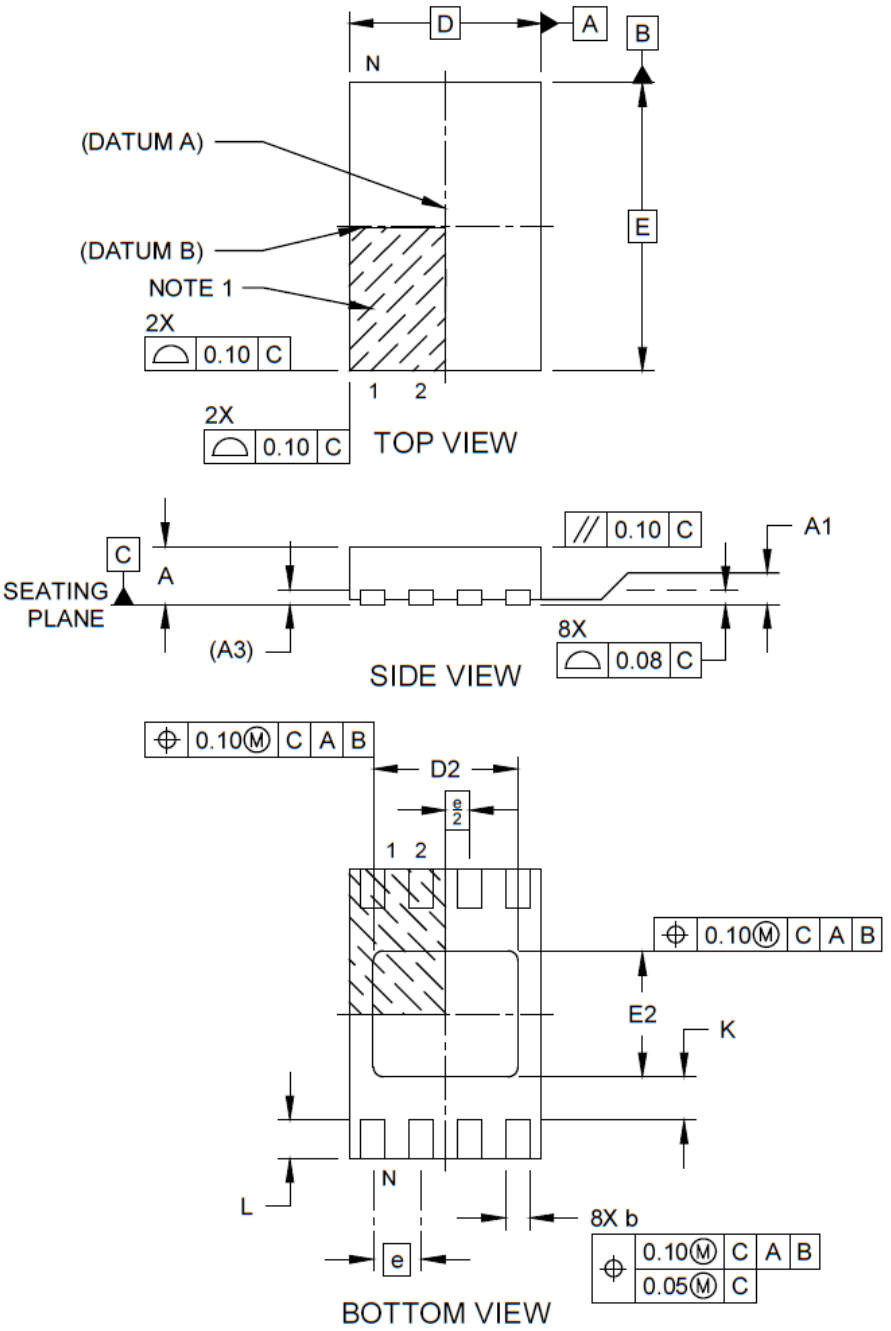
8.1 パッケージのマーキング情報

Microchip 社の全体的なセキュリティ対応の一環として、全ての暗号デバイスの製品マーキングは意図的に曖昧にされています。パッケージ上面のマークは、デバイスのタイプやデバイスの製造者に関する情報を一切提供しません。パッケージ上の英数字コードは製造情報を提供し、アセンブリロットに応じて異なります。受領検査時は、パッケージのマーキングに頼らない事を推奨します。

8.2 8 ピン UDFN

8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN]
Atmel Legacy Global Package Code YNZ

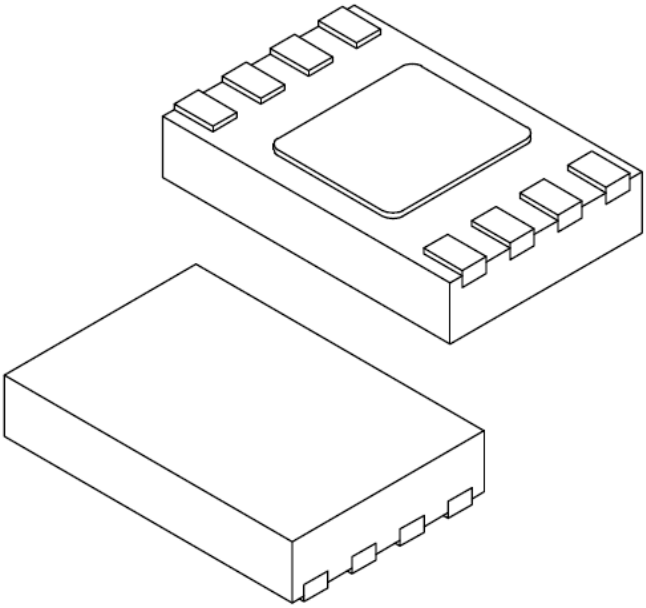
Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-21355-Q4B Rev B Sheet 1 of 2

8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN]
Atmel Legacy Global Package Code YNZ

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Terminals	N		8	
Pitch	e		0.50 BSC	
Overall Height	A	0.50	0.55	0.60
Standoff	A1	0.00	0.02	0.05
Terminal Thickness	A3		0.152 REF	
Overall Length	D		2.00 BSC	
Exposed Pad Length	D2	1.40	1.50	1.60
Overall Width	E		3.00 BSC	
Exposed Pad Width	E2	1.20	1.30	1.40
Terminal Width	b	0.18	0.25	0.30
Terminal Length	L	0.35	0.40	0.45
Terminal-to-Exposed-Pad	K	0.20	-	-

Notes:

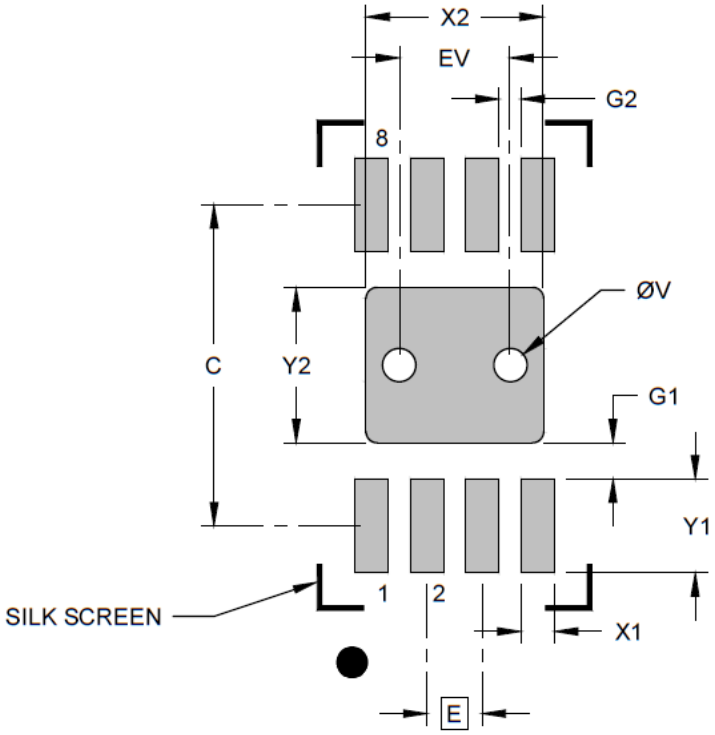
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.
REF: Reference Dimension, usually without tolerance, for information purposes only.

Microchip Technology Drawing C04-21355-Q4B Rev B Sheet 2 of 2

8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN]
Atmel Legacy Global Package Code YNZ

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		0.50 BSC	
Optional Center Pad Width	X2			1.60
Optional Center Pad Length	Y2			1.40
Contact Pad Spacing	C		2.90	
Contact Pad Width (X8)	X1			0.30
Contact Pad Length (X8)	Y1			0.85
Contact Pad to Center Pad (X8)	G1	0.33		
Contact Pad to Contact Pad (X6)	G2	0.20		
Thermal Via Diameter	V		0.30	
Thermal Via Pitch	EV		1.00	

Notes:

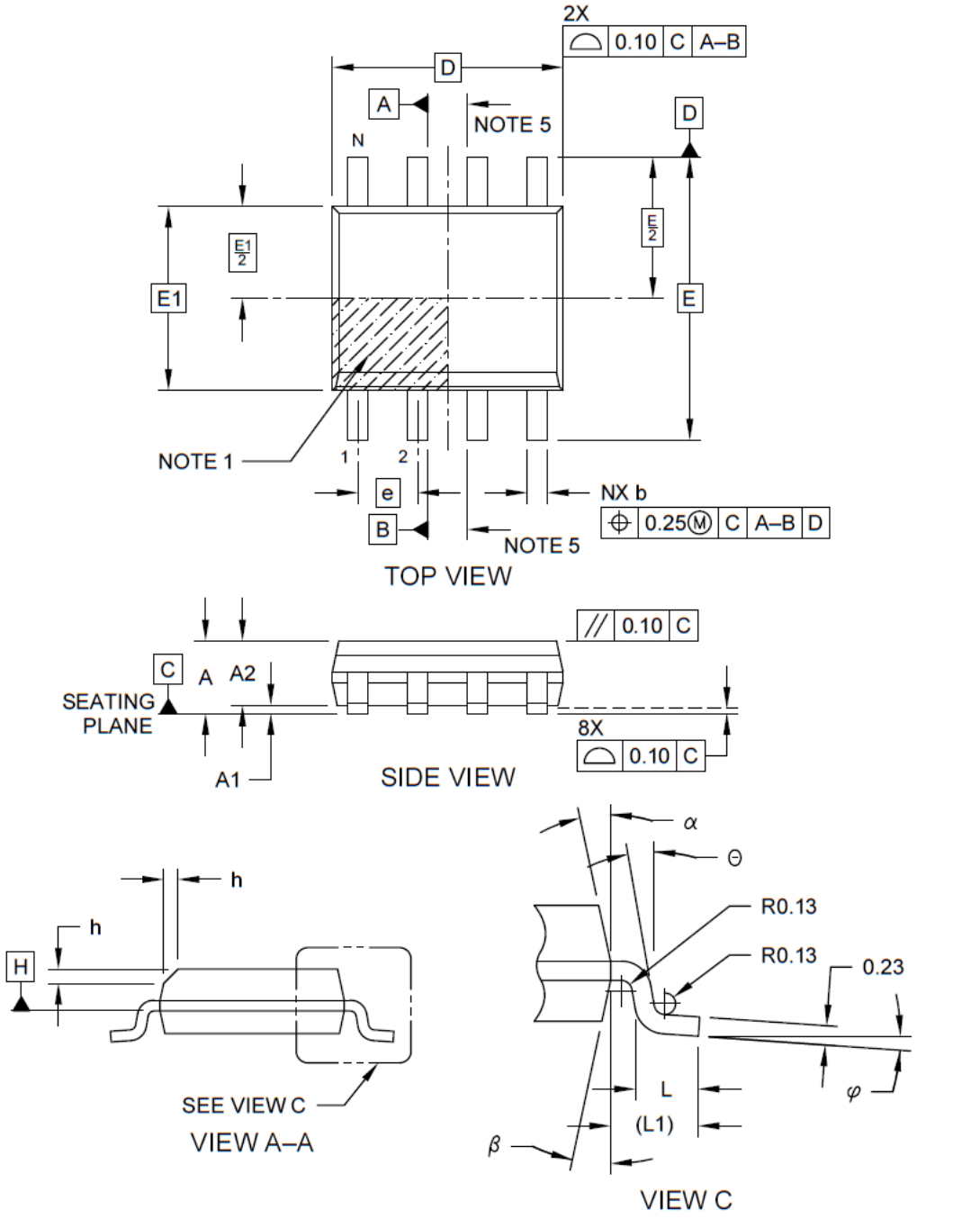
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

Microchip Technology Drawing C04-23355-Q4B Rev B

8.3 8 ピン SOIC

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy Global Package Code SWB

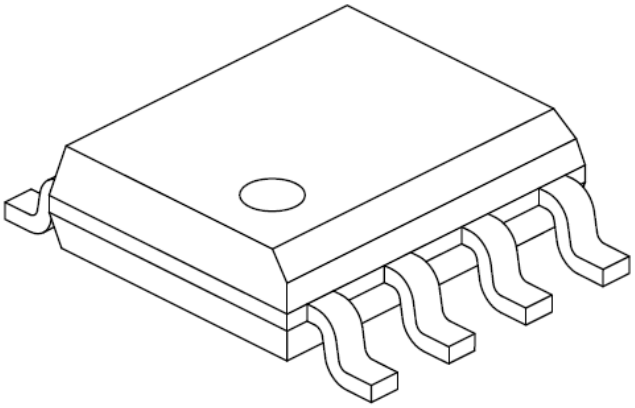
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing No. C04-057-SWB Rev E Sheet 1 of 2

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy Global Package Code SWB

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Pins	N		8	
Pitch	e		1.27 BSC	
Overall Height	A	-	-	1.75
Molded Package Thickness	A2	1.25	-	-
Standoff §	A1	0.10	-	0.25
Overall Width	E		6.00 BSC	
Molded Package Width	E1		3.90 BSC	
Overall Length	D		4.90 BSC	
Chamfer (Optional)	h	0.25	-	0.50
Foot Length	L	0.40	-	1.27
Footprint	L1		1.04 REF	
Foot Angle	φ	0°	-	8°
Lead Thickness	c	0.17	-	0.25
Lead Width	b	0.31	-	0.51
Mold Draft Angle Top	α	5°	-	15°
Mold Draft Angle Bottom	β	5°	-	15°

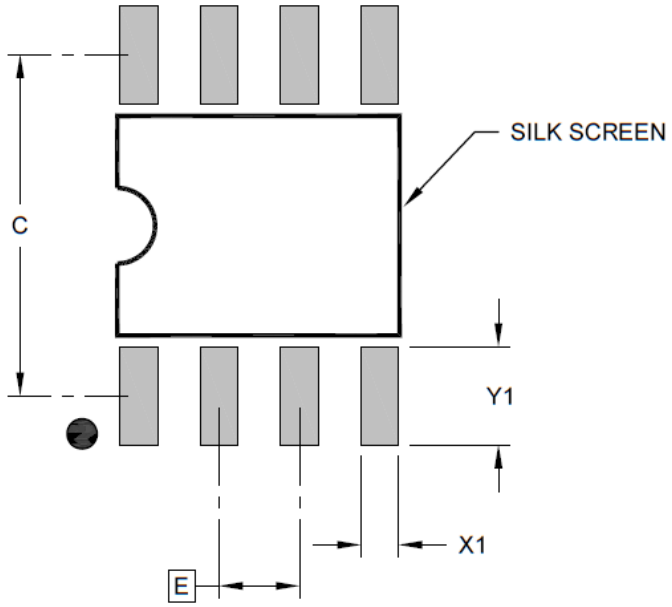
Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. § Significant Characteristic
3. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15mm per side.
4. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information purposes only.
5. Datums A & B to be determined at Datum H.

Microchip Technology Drawing No. C04-057-SWB Rev E Sheet 2 of 2

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy Global Package Code SWB

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		1.27 BSC	
Contact Pad Spacing	C		5.40	
Contact Pad Width (X8)	X1			0.60
Contact Pad Length (X8)	Y1			1.55

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-2057-SWB Rev E

9. 改訂履歴

リビジョン A (2021 年 9 月)
本書は初版です。

Microchip 社のウェブサイト

Microchip 社はウェブサイト(www.microchip.com)を通してオンライン サポートを提供しています。当ウェブサイトでは、お客様に役立つ情報やファイルを簡単に見つけ出せます。以下を含む各種の情報をご覧になれます。

- **製品サポート** - データシートとエラッタ、アプリケーション ノートとサンプル プログラム、設計リソース、ユーザガイドとハードウェア サポート文書、最新のソフトウェアと過去のソフトウェア
- **技術サポート** – FAQ(よく寄せられる質問)、技術サポートのご依頼、オンライン ディスカッション グループ、Microchip 社のデザイン パートナー プログラムおよびメンバーリスト
- **ご注文とお問い合わせ** - 製品セレクタと注文ガイド、最新プレスリリース、セミナー/イベントの一覧、お問い合わせ先(営業所/正規代理店)の一覧

製品変更通知サービス

Microchip 社の製品変更通知サービスは、お客様に Microchip 社製品の最新情報をお届けする配信サービスです。ご興味のある製品ファミリまたは開発ツールに関する変更、更新、リビジョン、エラッタ情報をいち早くメールにてお知らせします。

http://www.microchip.com/pcn にアクセスし、登録手続きをしてください。

カスタマサポート

Microchip 社製品をお使いのお客様は、以下のチャンネルからサポートをご利用になれます。

- 正規代理店
- 技術サポート

サポートは販売代理店にお問い合わせください。各地の営業所もご利用になれます。本書の最後のページに各国の営業所の一覧を記載しています。

技術サポートは以下のウェブページからもご利用になれます。技術サポート

製品識別システム

ご注文や製品の価格、納期につきましては弊社正規代理店にお問い合わせください。

製品番号	X	-X
デバイス	パッケージ タイプ	テープ&リール

デバイス:	ECC608-TFLXWPC: セキュアなハードウェア ベース鍵ストレージを備えた設定済み暗号コプロセッサ	
パッケージ オプション	U	8 ピン 2 x 3 x 0.6 mm ボディ、 熱的に強化された Plastic Ultra Thin Dual Flat (UDFN) 鉛フリー パッケージ
	S	8 ピン(0.150"幅ボディ)、Plastic Gull Wing Small Outline (JEDEC® SOIC)
テープ&リール オプション		2K リール
	PROTO	10 ユニットバルク - プロトタイプ ユニット

例:

- ECC608-TFLXWPCU:
  TrustFLEX TLS、プロビジョニング済み、8-UDFN、2K 個リール MOQ、I²C インターフェイス
- ECC608-TFLXWPCU-PROTO:
  TrustFLEX TLS、プロビジョニング済みプロトタイプ、8-UDFN, 10 個バルク、SWI または I²C インターフェイス
- ECC608-TFLXWPCS:
  TrustFLEX TLS、プロビジョニング済み、8-SOIC、2K 個リール MOQ、I²C インターフェイス
- ECC608-TFLXWPCS-PROTO:
  TrustFLEX TLS、プロビジョニング済みプロトタイプ、8-SOIC, 10 個バルク、I²C インターフェイス

Note:

1. テープ&リールの識別情報はカタログの製品番号説明にのみ記載しています。これは製品の注文時に使う識別情報であり、デバイスのパッケージには印刷していません。テープ&リールが選択できるパッケージの在庫/供給状況は正規代理店にお問い合わせください。

Microchip 社のデバイスコード保護機能

Microchip 社製品のコード保護機能について以下の点にご注意ください。

- Microchip 社製品は、該当する Microchip 社データシートに記載の仕様を満たしています。
- Microchip 社では、通常の条件ならびに仕様に従って使った場合、Microchip 社製品のセキュリティ レベルは、現在市場に流通している同種製品の中でも最も高度であると考えています。
- Microchip 社はその知的財産権を重視し、積極的に保護しています。Microchip 社製品のコード保護機能の侵害は固く禁じられており、デジタル ミレニアム著作権法に違反します。
- Microchip 社を含む全ての半導体メーカーで、自社のコードのセキュリティを完全に保証できる企業はありません。コード保護機能とは、Microchip 社が製品を「解読不能」として保証するものではありません。コード保護機能は常に進歩しています。Microchip 社では、常に製品のコード保護機能の改善に取り組んでいます。

法律上の注意点

本書および本書に記載されている情報は、Microchip 社製品を設計、テスト、お客様のアプリケーションと統合する目的を含め、Microchip 社製品に対してのみ使用する事ができます。それ以外の方法でこの情報を使用する事はこれらの条項に違反します。デバイス アプリケーションの情報は、ユーザの便宜のためにのみ提供されるものであり、更新によって変更となる事があります。お客様のアプリケーションが仕様を満たす事を保証する責任は、お客様にあります。その他のサポートは Microchip 社正規代理店にお問い合わせ頂くか、www.microchip.com/en-us/support/design-help/client-support-services をご覧ください。

Microchip 社は本書の情報を「現状のまま」で提供しています。Microchip 社は、明示的、暗黙的、書面、口頭、法定のいずれであるかを問わず、本書に記載されている情報に関して、状態、品質、性能、商品性、特定目的への適合性をはじめとする、いかなる類の表明も保証も行いません。

いかなる場合も Microchip 社は、本情報またはその使用に関連する間接的、特殊的、懲罰的、偶発、的または必然的損失、損害、費用、経費のいかんにかかわらず、また Microchip 社がそのような損害が生じる可能性について報告を受けていた場合あるいは損害が予測可能であった場合でも、一切の責任を負いません。法律で認められる最大限の範囲を適用しようとも、本情報またはその使用に関連する一切の申し立てに対する Microchip 社の責任限度額は、使用者が当該情報に関連して Microchip 社に直接支払った額を超えません。

Microchip 社の明示的な書面による承認なしに、生命維持装置あるいは生命安全用途に Microchip 社の製品を使用する事は全て購入者のリスクとし、また購入者はこれによって発生したあらゆる損害、クレーム、訴訟、費用に関して、Microchip 社は擁護され、免責され、損害をうけない事に同意するものとします。特に明記しない場合、暗黙的あるいは明示的を問わず、Microchip 社が知的財産権を保有しているライセンスは一切譲渡されません。

商標

Microchip 社の名称とロゴ、Microchip ロゴ、Adaptec、AnyRate、AVR、AVR ロゴ、AVR Freaks、BesTime、BitCloud、CryptoMemory、CryptoRF、dsPIC、flexPWR、HELDO、IGLOO、JukeBlox、KeeLoq、Kleer、LANCheck、LinkMD、maXStylus、maXTouch、MediaLB、megaAVR、Microsemi、Microsemi ロゴ、MOST、MOST ロゴ、MPLAB、OptoLyzer、PIC、picoPower、PICSTART、PIC32 ロゴ、PolarFire、Prochip Designer、QTouch、SAM-BA、SenGenuity、SpyNIC、SST、SST ロゴ、SuperFlash、Symmetricom、SyncServer、Tachyon、TimeSource、tinyAVR、UNI/O、Vectron、XMEGA は米国およびその他の国における Microchip Technology Incorporated の登録商標です。

AgileSwitch、APT、ClockWorks、The Embedded Control Solutions Company、EtherSynch、Flashtec、Hyper Speed Control、HyperLight Load、IntelliMOS、Libero、motorBench、mTouch、Powermite 3、Precision Edge、ProASIC、ProASIC Plus、ProASIC Plus ロゴ、Quiet-Wire、SmartFusion、SyncWorld、Temux、TimeCesium、TimeHub、TimePictra、TimeProvider、TrueTime、WinPath、ZL は米国における Microchip Technology Incorporated の登録商標です。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、Augmented Switching、BlueSky、BodyCom、CodeGuard、CryptoAuthentication、CryptoAutomotive、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、Espresso T1S、EtherGREEN、GridTime、IdealBridge、In-Circuit Serial Programming、ICSP、INICnet、Intelligent Paralleling、Inter-Chip Connectivity、JitterBlocker、Knob-on-Display、maxCrypto、maxView、memBrain、Mindi、MiWi、MPASM、MPF、MPLAB Certified ロゴ、MPLIB、MPLINK、MultiTRAK、NetDetach、NVM Express、NVMe、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、PowerSmart、PureSilicon、QMatrix、REAL ICE、Ripple Blocker、RTAX、RTG4、SAM- ICE、Serial Quad I/O、simpleMAP、SimpliPHY、SmartBuffer、SmartHLS、SMART-I.S.、storClad、SQI、SuperSwitcher、SuperSwitcher II、Switchtec、SynchroPHY、Total Endurance、TSHARC、USBCheck、VariSense、VectorBlox、VeriPHY、ViewSpan、WiperLock、XpressConnect、ZENA は米国およびその他の国における Microchip Technology Incorporated の商標です。

SQTP は米国における Microchip Technology Incorporated のサービス マークです。

Adaptec ロゴ、Frequency on Demand、Silicon Storage Technology、Symmcom、Trusted Time はその他の国における Microchip Technology Incorporated の登録商標です。

GestIC は、米国以外の国における Microchip Technology Inc.の子会社である Microchip Technology Germany II GmbH & Co. KG の登録商標です。

その他の商標は各社に帰属します。

ISBN: 978-1-6683-0256-9

品質管理システム

Microchip 社の品質管理システムについては www.microchip.com/quality をご覧ください。

各国の営業所とサービス

北米

本社
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel:480-792-7200
Fax:480-792-7277
技術サポート：
http://www.microchip.com/support
URL:
www.microchip.com

アトランタ
Duluth, GA
Tel:678-957-9614
Fax:678-957-1455

オースティン、TX
Tel:512-257-3370

ボストン
Westborough, MA
Tel:774-760-0087
Fax:774-760-0088

シカゴ
Itasca, IL
Tel:630-285-0071
Fax:630-285-0075

ダラス
Addison, TX
Tel:972-818-7423
Fax:972-818-2924

デトロイト
Novi, MI
Tel:248-848-4000

ヒューストン、TX
Tel:281-894-5983

インディアナポリス
Noblesville, IN
Tel:317-773-8323
Fax:317-773-5453
Tel:317-536-2380

ロサンゼルス
Mission Viejo, CA
Tel:949-462-9523
Fax:949-462-9608
Tel:951-273-7800

ローリー、NC
Tel:919-844-7510

ニューヨーク、NY
Tel:631-435-6000

サンノゼ、CA
Tel:408-735-9110
Tel:408-436-4270

カナダ - トロント
Tel:905-695-1980
Fax:905-695-2078

アジア /太 平洋

オーストラリア - シドニー
Tel:61-2-9868-6733

中国 - 北京
Tel:86-10-8569-7000

中国 - 成都
Tel:86-28-8665-5511

中国 - 重慶
Tel:86-23-8980-9588

中国 - 東莞
Tel:86-769-8702-9880

中国 - 広州
Tel:86-20-8755-8029

中国 - 杭州
Tel:86-571-8792-8115

中国 - 香港 SAR
Tel:852-2943-5100

中国 - 南京
Tel:86-25-8473-2460

中国 - 青島
Tel:86-532-8502-7355

中国 - 上海
Tel:86-21-3326-8000

中国 - 瀋陽
Tel:86-24-2334-2829

中国 - 深圳
Tel:86-755-8864-2200

中国 - 蘇州
Tel:86-186-6233-1526

中国 - 武漢
Tel:86-27-5980-5300

中国 - 西安
Tel:86-29-8833-7252

中国 - 厦門
Tel:86-592-2388138

中国 - 珠海
Tel:86-756-3210040

アジア /太 平洋

インド - バンガロール
Tel:91-80-3090-4444

インド - ニューデリー
Tel:91-11-4160-8631

インド - プネ
Tel:91-20-4121-0141

日本 - 大阪
Tel:81-6-6152-7160

日本 - 東京
Tel:81-3-6880- 3770

韓国 - 大邱
Tel:82-53-744-4301

韓国 - ソウル
Tel:82-2-554-7200

マレーシア - クアラルンプール
Tel:60-3-7651-7906

マレーシア - ペナン
Tel:60-4-227-8870

フィリピン - マニラ
Tel:63-2-634-9065

シンガポール
Tel:65-6334-8870

台湾 - 新竹
Tel:886-3-577-8366

台湾 - 高雄
Tel:886-7-213-7830

台湾 - 台北
Tel:886-2-2508-8600

タイ - バンコク
Tel:66-2-694-1351

ベトナム - ホーチミン
Tel:84-28-5448-2100

ヨーロッパ

オーストリア - ヴェルス
Tel:43-7242-2244-39
Fax:43-7242-2244-393

デンマーク - コペンハーゲン
Tel:45-4485-5910
Fax:45-4485-2829

フィンランド - エスポー
Tel:358-9-4520-820

フランス - パリ
Tel:33-1-69-53-63-20
Fax:33-1-69-30-90-79

ドイツ - ガーヒング
Tel:49-8931-9700

ドイツ - ハーン
Tel:49-2129-3766400

ドイツ - ハイルブロン
Tel:49-7131-72400

ドイツ - カールスルーエ
Tel:49-721-625370

ドイツ - ミュンヘン
Tel:49-89-627-144-0
Fax:49(-89/-627)-144/-44

ドイツ - ローゼンハイム
Tel:49-8031-354-560

イスラエル - ラーナナ
Tel:972-9-744-7705

イタリア - ミラノ
Tel:39-0331-742611
Fax:39-0331-466781

イタリア - パドヴァ
Tel:39-049-7625286

オランダ - ドリューネン
Tel:31-416-690399
Fax:31-416-690340

ノルウェー - トロンハイム
Tel:47-7288-4388

ポーランド - ワルシャワ
Tel:48-22-3325737

ルーマニア - ブカレスト
Tel:40-21-407-87-50

スペイン - マドリッド
Tel:34-91-708-08-90
Fax:34-91-708-08-91

スウェーデン - ヨーテボリ
Tel:46-31-704-60-40

スウェーデン - ストックホルム
Tel:46-8-5090-4654

イギリス - ウォーキンガム
Tel:44-118-921-5800
Fax:44-118-921-5820