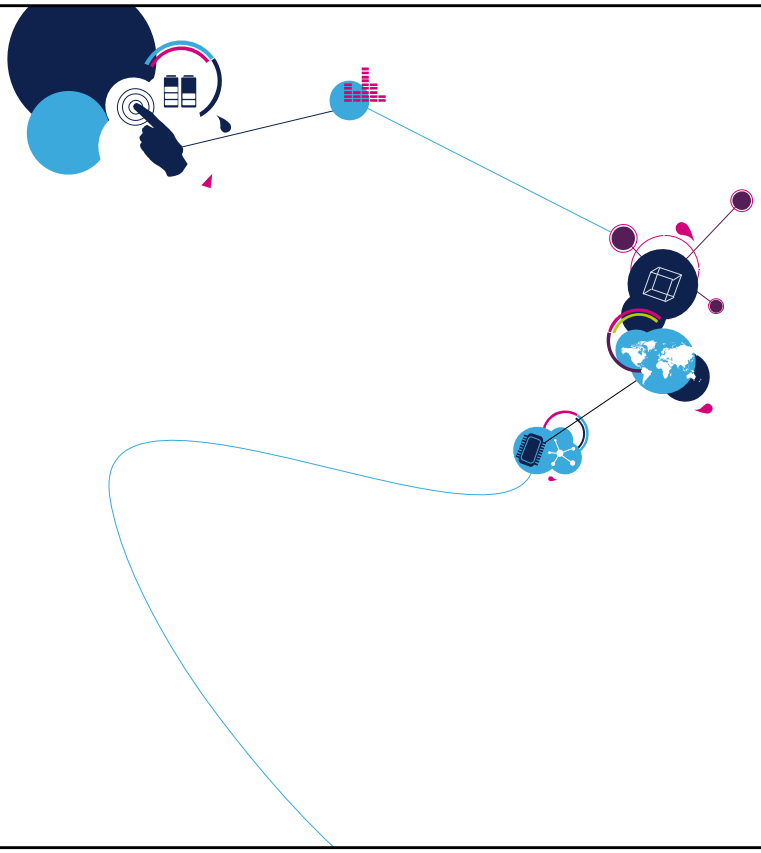
STM32G0 – DES
デバイス電子署名



レビジョン 1.0

life.augmented

デバイス識別またはシリアル番号として使用できる STM32 デバイス電子署名のプレゼンテーションへようこそ。

概要

- デバイス電子署名によってアプリケーションが読み出すことができる一意の下記デバイス情報を提供
  - 96ビット長のユニークID（UID）
  - Flashメモリ・サイズとパッケージ・タイプ情報

アプリケーション側の利点

- セキュリティおよびシリアル番号体系にユニーク・デバイス識別子を使用可能
- マルチプラットフォーム・ファームウェア用のデバイス設定情報
- 読出し専用情報
- 使用および実装が容易

life.augmented

デバイスの電子署名によって、ダイ ID、ユニークデバイス識別子（UID）、およびメモリサイズ、パッケージタイプ、デバイス較正情報などのその他の読出し専用デバイス情報を格納したレジスタセットが提供されます。
アプリケーションは、シリアル番号またはセキュリティキーの一部として使用できるユニーク識別子のメリットを活用できます。また、UID に基づいてソフトウェア配布／ライセンス機能を管理するためにも使用できます。

主な機能

STからの出荷時に事前プログラム済み

- STからの出荷時に事前プログラムされたUID
  - ユーザは変更できない
- デバイス情報データ
  - Flashメモリ・サイズ
  - パッケージ・タイプ

アプリケーション側の利点

- シリアル番号またはセキュリティ・キーの一部として使用可能
- ソフトウェア・ライセンス処理：特定のUID範囲を使用して、出荷したファームウェアの機能／特徴を制限可能
- アプリケーションは、マルチプラットフォーム・ファームウェアで使用した場合、パッケージ・タイプとメモリ・サイズを決定可能

life.augmented

ユニーク識別子（UID）およびその他のデバイス情報は、STからの出荷時に事前にプログラムされており、ユーザが変更することはできません。この識別子は、セキュリティキーまたはシリアル番号、およびソフトウェアライセンス処理のための識別子として使用できます。マルチプラットフォームファームウェアでは、UID を使用して、アプリケーションの機能と特徴を管理するためのパッケージタイプとメモリサイズを決定できます。

ユニーク·デバイスIDレジスタ

4

読出し専用ユニーク·デバイス識別子

- ユニーク·デバイスIDは以下で構成される96ビットのレジスタ
  - ウェハ上のXおよびY座標
  - ロット番号とウェハ番号
- ユニークIDはデバイスごとに一意の識別子
- ユニーク·デバイスIDのすべてのビットが使用されるわけではない
  - レジスタに書き込まれたデータには、専用レジスタの幅よりも小さい限定された範囲(XおよびY座標など)がある
    - 特定のデバイスの「0」に「固定」されていない有効なビットに関する正確な情報は、リクエストに応じて入手可能
  - レジスタの一部のビットは、特定の製品に対して常に「0」
  - セキュリティ関連のアプリケーションは、UIDの一部のみを使用してセキュリティ·キーを作成可能

life.augmented

ユニークデバイス識別子は、ウェハ上のダイの座標、ロット番号、およびウェハ番号を含む 96 ビットのレジスタです。
この識別子は ST が製造したデバイスごとに一意です。
ユニーク識別子内の各レコードには、X 座標と Y 座標のような特定の範囲があるため、デバイス ID のすべてのビットが使用されるわけではありません。これは、使用されるビット数が重要なパラメータであるセキュリティ関連の目的にとって重要です。このようなセキュリティアプリケーションは、デバイス ID の一部しか使用できません。また、「固定」ビットは使用しないでください。

参照

- 詳細については、次のソースを参照：
  - STM32G0xx MCUリファレンスマニュアル

詳細については、デバイスのリファレンスマニュアルとデータシートを参照してください。