

# STM32G4 – DES デバイス電子署名

1.0版



こんにちは。デバイスのID、またはシリアル番号として使用することができるSTM32デバイス電子署名のプレゼンテーションへようこそ。



- デバイス電子署名によってアプリケーションが読み出せ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)
  - 部品番号の符号とパッケージ・タイプの情報

### アプリケーション側の利点

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

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、デバイス校正情報などのその他の読取り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恩恵を受けることができます。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。

## STのファクトリで事前プログラム済み

- STのファクトリで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
- 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、デバイスの部品番号、バージョン、パッケージタイプを取得



ユニーク識別子 (UID) およびその他のデバイス情報は、STのファクトリで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、デバイス情報を使用して、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部品番号を判断できます。

# ユニーク・デバイスIDレジスタ

4

## 読出し専用のユニーク・デバイス識別子

- ユニーク・デバイスIDは下記から成る96ビットのレジスタ
  - ウェハ上のXおよびY座標
  - ロットおよびウェハ番号
- ユニークIDはデバイスごとに一意な識別子
- 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(たとえば、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、ユニークIDをハッシュしてセキュリティ・キーを作成可能



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。

- 詳細は以下の資料をご参照ください。:
  - STM32G4xx MCU reference manuals



life.augmented

詳細情報については、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。