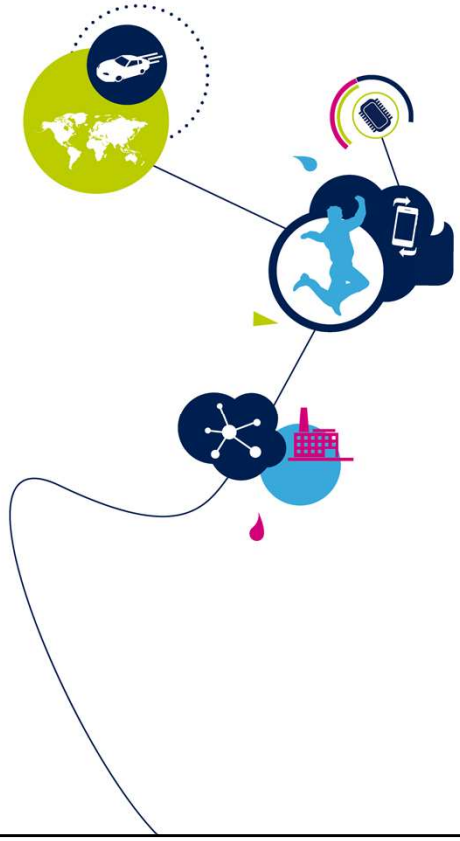
STM32H7 – DES

デバイス電子署名

1.0版



life.augmented

デバイスID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(Device Electronic Signature: DES) のプレゼンテーションにようこそ。

概要

- デバイス電子署名は、アプリケーションから読み出し可能な、次のようなユニークなデバイス情報を提供
  - 96ビット長ユニークID（UID）
  - Flashメモリ・サイズとパッケージ・タイプの情報

アプリケーション側の利点

- ユニークなデバイス識別子は、セキュリティとシリアル番号スキームのために使用可能
- マルチプラットフォーム・ファームウェア用のデバイス設定情報
- 読出し専用情報
- 使用と実装が容易

life.augmented

デバイス電子署名は、ダイ識別、ユニークデバイス識別子（UID）と、メモリサイズ、パッケージタイプ、デバイス較正情報などその他の読出し専用デバイス情報が含まれるレジスタのセットを提供します。
アプリケーションは、シリアル番号として、あるいはセキュリティキーの一部として使用できるユニークな識別子を活用できます。また、UIDに基づくソフトウェア配布／ライセンシング機能の管理にも使用できます。

主な機能

STの工場で事前にプログラム済み

- STの工場で事前にプログラム済みのUID
  - ユーザによる変更不可
- 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

- シリアル番号として、あるい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･ライセンシング： 特定のUID範囲を使用して、納入ファームウェアの機能／特徴を制限可能
- マルチプラットフォーム･ファームウェアで使用された場合に、アプリケーションがパッケージ･タイプとメモリ･サイズを識別可能

life.augmented

ユニークな識別子とその他のデバイス情報がSTの工場で事前にプログラムされており、ユーザは変更できません。この識別子は、セキュリティキーまたはシリアル番号として、そしてソフトウェアライセンシング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は、アプリケーションの機能と特徴を管理するために、UIDを使用してパッケージタイプとメモリサイズを識別できます。

ユニークデバイスIDレジスタ

4

読出し専用のユニークなデバイス識別子

- ユニークデバイスIDは、次の情報から構成される96ビットのレジスタ
  - ウェハ上のXおよびY座標
  - ロットとウェハ番号
- ユニークIDは各デバイスにユニークな識別子
- ユニークデバイスIDのすべてのビットが使用されている訳ではない
  - 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狭い限定範囲（X座標とY座標など）がある
    - ある特定のデバイスに対する‘0’に「固定」されていない有効ビットに関する情報は、リクエストに応じて提供可能
  - レジスタ内の特定のビットは、ある特定のデバイスに対して常に‘0’となる
  - セキュリティ関連アプリケーションは、UIDの一部のみを用いてセキュリティキーを生成可能

life.augmented

ユニークデバイス識別子は、ウェハ上のダイ座標、ロット番号、ウェハ番号が含まれている96ビットレジスタです。
この識別子は、ST が製造するデバイスごとにユニークです。ユニーク識別子の中の各レコードには、X座標とY座標のようなある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ている訳ではありません。このことは、使用されてい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は重要です。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の一部のみを使用可能であり、「固定」ビットの使用を避けることが望まれます。

参照

- 詳細については、以下のソースをご参照ください
  - STM32H7 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ご参照ください。