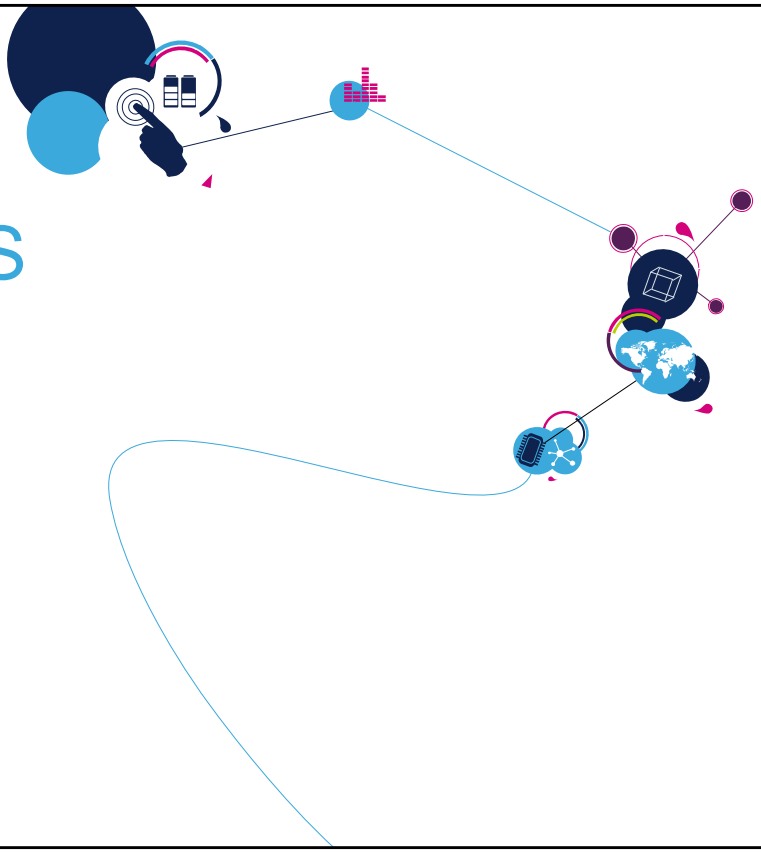

STM32MP1 - DES
デバイス電子署名

1.0 版

life.augmented

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せる一意の下記デバイス情報を提供
  - 96bit 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

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。

主な特徴

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
  - デバイスの部品番号およびバージョン
  - 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

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 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 96bit 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
  - 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

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 96bit 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ーであるセキュリティ関連の目的にとって重要です。そのようなセキュリティアプリケーションでは、ユニーク ID をハッシュしてセキュリティキーを作成することができます。

参照

- 詳細については、以下のソースを参照可能
  - STM32MP1 リファレンスマニュアル（RM0441、RM0442、RM0436）

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。