暗号ファームウェアライブラリのプレゼンテーションへようこそ。

U5 の ST 暗号ライブラリ – 主な変更点 認証済み NIST CAVP

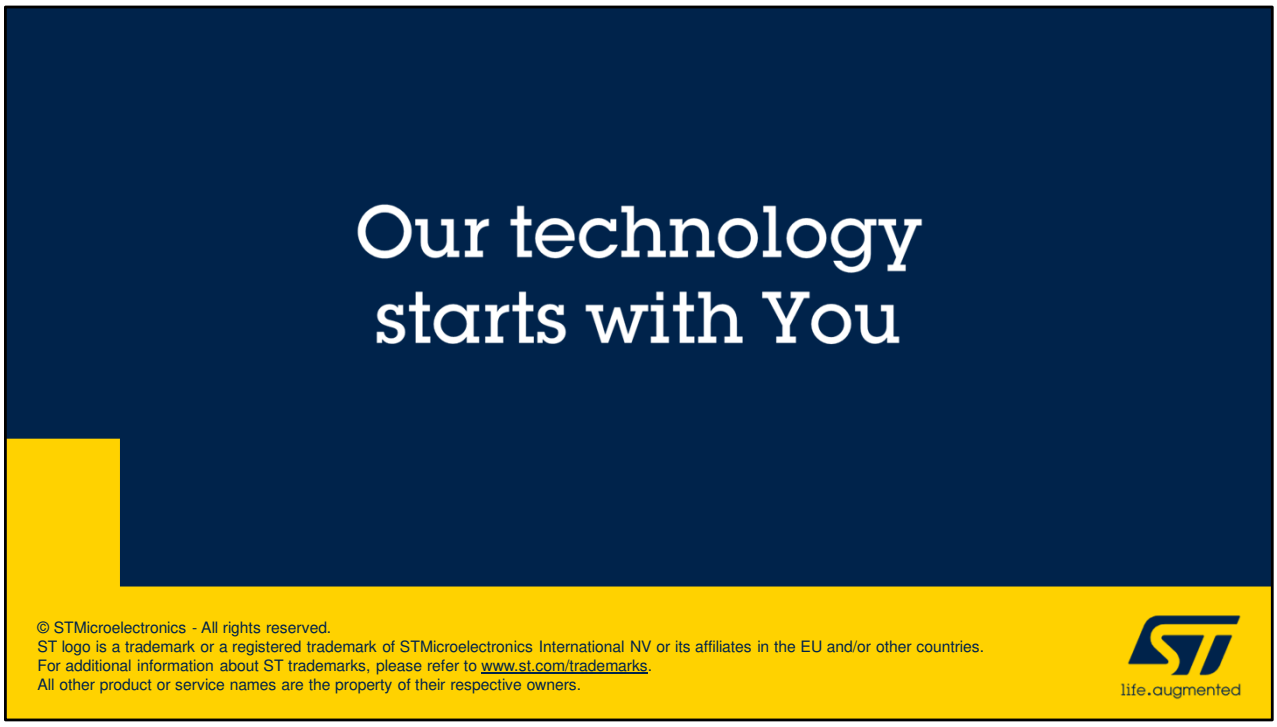
STM32 マイクロコントローラのすべてのコアに準拠した U5 の暗号ライブラリ V4.xx

- 新しい暗号化アルゴリズム（SM2/3/4、SHA、RSA CRT）
- 認証済み NIST CAVP
  - 参照先 https://wiki.st.com/stm32mcu/wiki/Security:Cryptographic_Library_Certifications
- ソフトウェアのモジュール性が改善された純粋なソフトウェア実装
- PSA 暗号化 API と同様のシンプルで新しい API
- メモリ・フットプリントの最適化
- 性能の最適化（Cortex-M アセンブリ命令を使用）
- X-Cube-CryptoLib バージョン 4.x.x で提供
  - https://www.st.com/en/embedded-software/x-cube-cryptolib.html を参照してください

life.augmented

2

STM32 暗号化ライブラリパッケージ（X-CUBE-CRYPTOLIB）には、暗号化、ハッシュ、メッセージの認証、デジタル署名に使用される主要なセキュリティアルゴリズムがすべて含まれ、開発者は、データの整合性、機密性、識別/認証、および否認防止のあらゆる組み合わせに関する適用要件を満たすことができます。
アメリカ国立標準技術研究所（NIST） 暗号アルゴリズム検証プログラム（CAVP）では、承認された暗号化アルゴリズムとその個別の構成要素の検証テストに対応します。
ST 暗号ライブラリは、NIST CAVP によって認証されています。
このスライドでは、STM32U5 で使用可能なライブラリの主な変更点を示します。
新しい暗号化アルゴリズムとして、SM バージョン 2、3、および 4、SHA および RSA CRT がサポートされます。
ライブラリのモジュール性が改善されています。
PSA 暗号化 API と整合した新しい API を備えています。
アセンブリ言語で設計された一部の部品により、コードサイズと性能が最適化されます。
ライブラリは、X-Cube-CryptoLib バージョン 4.x.x で提供されます。



このプレゼンテーションにご参加いただき、ありがとうございました。