Hello, and welcome to this presentation of the cryptographic firmware library.

ST Crypto Library on STM32H5 Certified NIST CAVP

Cryptographic Library V4.x.x on H5 and compliant with all cores in STM32 MCUs

- Certified NIST CAVP
  - Refer to: https://wiki.st.com/stm32mcu/wiki/Security:Cryptographic_Library_Certifications
- Pure software implementation with improved software modularity
- Simpler + new API with similarity to PSA crypto API
- Memory footprint optimizations
- Performance optimizations (using Cortex-M assembly instructions)

life.augmented

2

The ST Crypto library is certified by NIST CAVP.
The National Institutes of Standards and Technology (NIST) Cryptographic Algorithm Validation Program (CAVP) provides validation testing of approved cryptographic algorithms and their individual components.
The modularity of the library has been improved.
It offers a new API, aligned with PSA crypto API.
Code size and performance are optimized, thanks to some parts designed in assembly language.

STM32 Cryptographic Firmware Library
Rich set of examples

Delivered in X-Cube-CryptoLib version 4.x.x

Refer to *https://www.st.com/en/embedded-software/x-cube-cryptolib.html*

- Cipher algorithms :
  - AES (modes CBC, CCM, CFB, CTR, ECB, GCM, OFB, XTS, Keywrap),
  - SM4, Chacha20-Poly1305
- Hash methods :
  - SHA-1, SHA-2, SHA-3, SM3, SHAKE
- Message Authentication Code :
  - CMAC, HMAC, KMAC
- ECC :
  - ECDH, ECDSA, EdDSA, SM2
- RSA :
  - PKCS#1 v1.5, PKCS#1 v2.2, Chinese remainder theorem (CRT) key representation
- DRBG

life.augmented

3

The STM32 cryptographic library package (X-CUBE-CRYPTOLIB) includes all the major security algorithms for encrypting, hashing, authenticating messages, and digital signing, enabling developers to satisfy application requirements for any combination of data integrity, confidentiality, identification/authentication, and non-repudiation,
The library is delivered in X-Cube-CryptoLib version 4.

The STM32 Cryptographic Firmware Library includes a set of cryptographic algorithms based on firmware implementation ready to use with all STM32 series. The main algorithms are :

- Cipher algorithms : AES (modes CBC, CCM, CFB,

CTR, ECB, GCM, OFB, XTS, Keywrap), SM4, Chacha20-Poly1305
- Hash methods : SHA-1, SHA-2, SHA-3, SM3, SHAKE
- Message Authentication Code : CMAC, HMAC, KMAC
- ECC : ECDH, ECDSA, EdDSA, SM2
- RSA : PKCS#1 v1.5, PKCS#1 v2.2, Chinese remainder theorem (CRT) key representation
- DRBG

The STM32 Cryptographic Firmware Library provides a rich set of examples covering the main features of main cryptographic algorithm.
It covers also the most common development tools.
Examples are available in source file format and provided with preconfigured projects for the supported boards.

Firmware download and reference documentation

- DB2660:
  - Databrief of STM32 Cryptographic library for STM32Cube
- Wiki pages for Cryptographic Library:
  - Overview, getting started, secure usage, performances, certification and migration guide

life.augmented

You can obtain additional information by:
-Reading the X-CUBE-CRYPTOLIB data brief, reference DB2660
-Consulting the dedicated wiki pages.

Thank you

life.augmented

Thank you for attending this presentation!