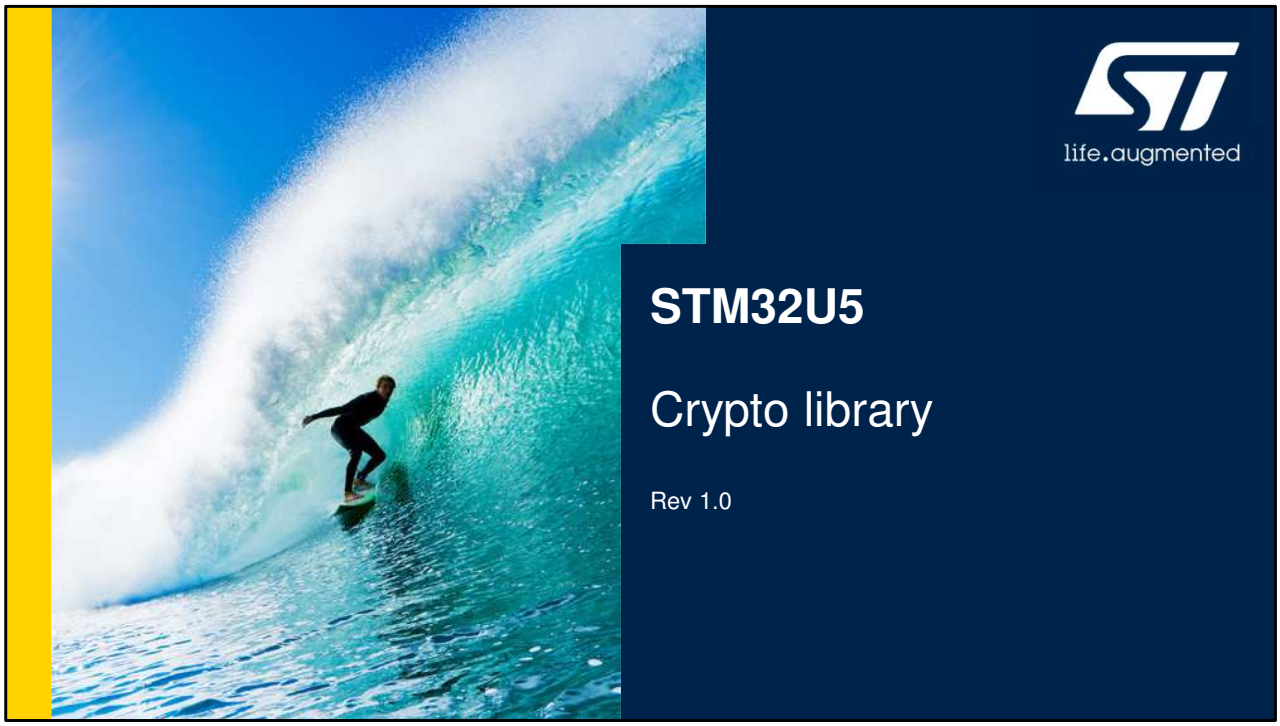

Hello, and welcome to this presentation of the cryptographic firmware library.

ST Crypto Library on U5 – Main changes Certified NIST CAVP

Cryptographic Library V4.x.x on U5 and compliant with all cores in STM32 MCUs

- New cryptographic algorithms (SM2/3/4, SHA, RSA CRT)
- 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)
- Delivered in X-Cube-CryptoLib version 4.x.x
  - Refer to https://www.st.com/en/embedded-software/x-cube-cryptolib.html

life.augmented

2

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 National Institutes of Standards and Technology (NIST) Cryptographic Algorithm Validation Program (CAVP) provides validation testing of approved cryptographic algorithms and their individual components. The ST Crypto library is certified by NIST CAVP.

This slide highlights the main changes made to the library available for STM32U5.

New cryptographic algorithms are supported: SM versions 2, 3 and 4, SHA and RSA CRT.
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.
The library is delivered in X-Cube-CryptoLib version 4.x.x.

Thank you

life.augmented

Thank you for attending this presentation!