X-CUBE-CRYPTOLIB

FIPS CAVP certification

life.augmented

X-CUBE-CRYPTOLIB

What is X-CUBE-CRYPTOLIB?

- a set of crypto algorithms based on ready-to-use firmware implementation in all STM32 microcontrollers
- Follows the STM32Cube architecture package
- For dedicated devices, some algorithms are supported with hardware acceleration
- software library classified ECCN 5D002
- provides examples covering all the available algorithms with template projects for the most widely used development tools:
  - Keil® MDK-ARM™
  - IAR Embedded Workbench® EWARM
  - AC6 SW4STM32
  - Atollic® TrueSTUDIO®
- available free of charge under our Software License Agreement (SLA)

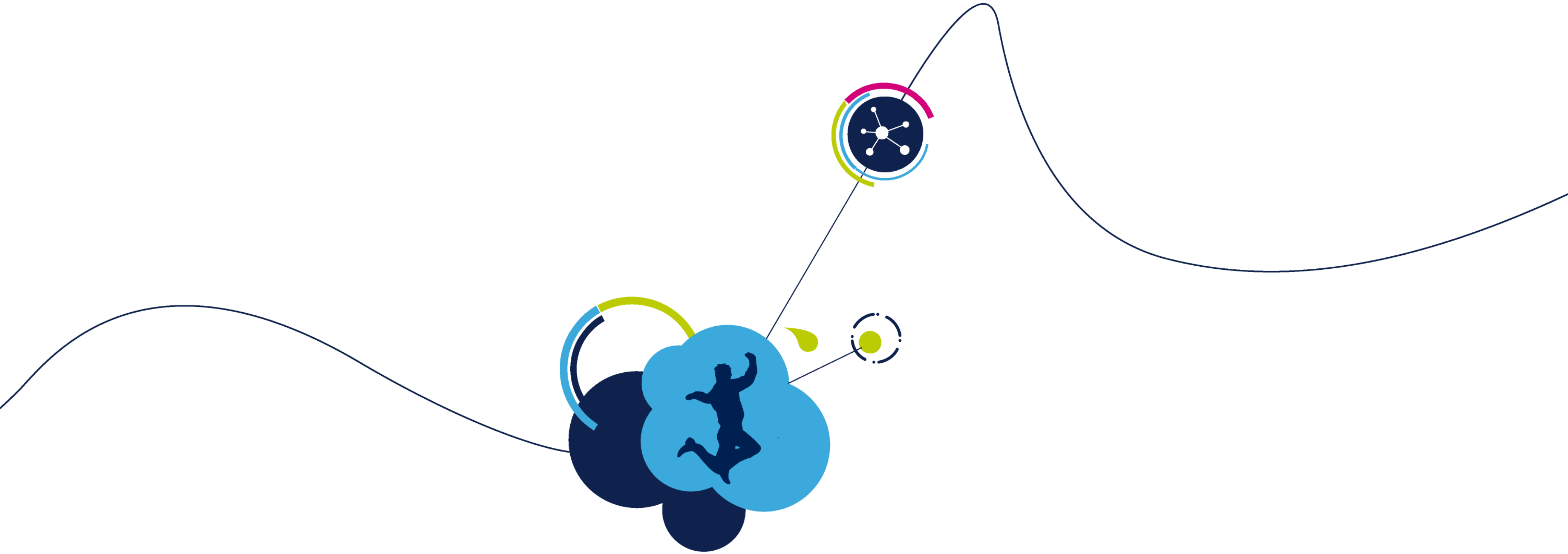
Find more on st.com

www.st.com/x-cube-cryptolib

Documentation: DB2660, UM1924, and license agreement SLA0048

Supported algorithms

- AES-128, AES-192, and AES-256
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher-Block Chaining) with support for ciphertext stealing
  - CTR (Counter Mode)
  - CFB (Cipher Feedback)
  - OFB (Output Feedback)
  - CCM (Counter with CBC-MAC)
  - GCM (Galois Counter Mode)
  - CMAC
  - KEY WRAP
  - XTS (XEX-based tweaked-codebook mode with ciphertext stealing)
- DES and TripleDES:
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher-Block Chaining)
- ARC4
- Random bit generator engine based on DRBG-AES-128
- Hash function: HKDF-SHA-512
- Hash functions with HMAC support:
  - MD5
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
- RSA with PKCS#1v1.5
  - Encryption/decryption
  - Signature
- ECC (Elliptic Curve Cryptography):
  - Key generation
  - Scalar multiplication (the base for ECDH)
  - ECDSA
- ChaCha20
- Poly1305
- Chacha20-Poly1305
- ED25519
- Curve25519



FIPS CAVP standard

NIST certification program

- Federal Information Processing Standard - FIPS 140
  - Defines requirements for cryptographic systems used in sensitive government systems
  - Defines 4 system security levels → for STM32 user applications
    - Level 1: Basic security requirements
    - Level 2: Physical tamper evidence, role-based authentication
    - Level 3: Enhanced physical security, user-based authentication
    - Level 4: Envelope and environmental protection

- 2 main validation programs:
  - Cryptographic Module Validation Program (CMVP)
  - Cryptographic Algorithm Validation Program (CAVP)

Established by the National Institute of Standards and Technology (NIST / US)
and the Communications Security Establishment (CSE / Canada) in 1995

Cryptographic Module Validation Program (CMVP)

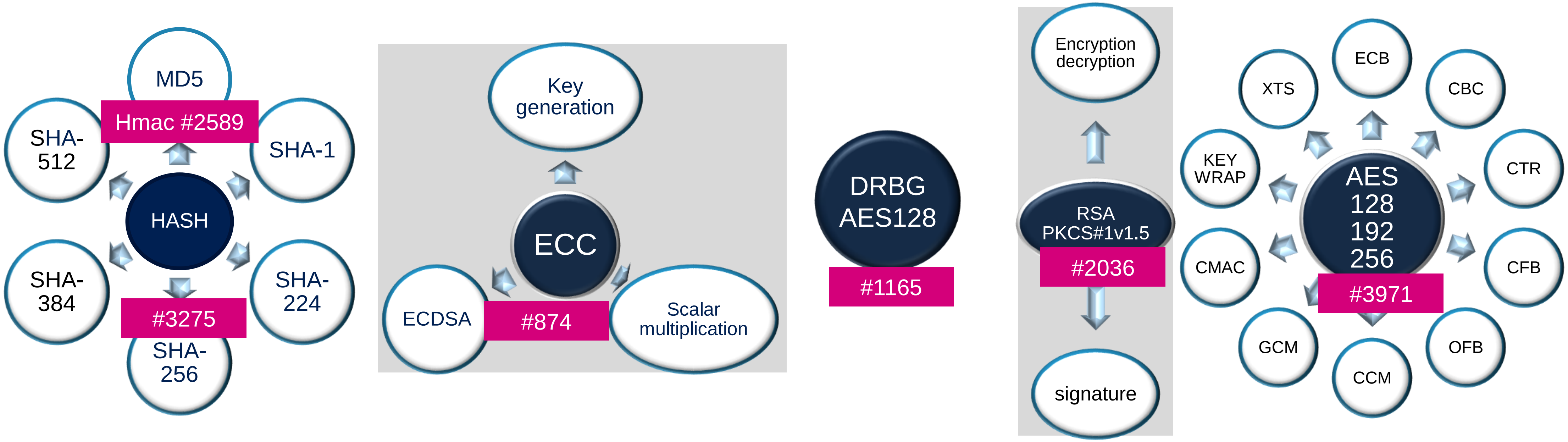
- Oversees the validation testing of cryptographic modules and algorithms
- Issues validation certificates
- Maintains a list of validated modules and algorithms for ST customers
  - SSL / TLS module
  - Key management service (HSM)
  - Secure Crypto Kernel OS
  - Gateway
  - Cryptographic server
  - JAVA OS
  - Wireless LAN module
  - Cloud router
  - PIV access control

Cryptographic Algorithm Validation Program (CAVP)

- Provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components
- Issues validation certificates
- Maintains a list of validated algorithms
- Validated **X-CUBE-CRYPTOLIB** algorithms for STM32
  - AES: #3971
  - RSA: #2036
  - ECDSA: #874
  - SHS: #3275
  - DRBG: #1165
  - HMAC: #2589

Cryptographic Algorithm Validation Program (CAVP)

- Provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components
  - Issues validation certificates
  - Maintains a list of validated algorithms
  - Validated **X-CUBE-CRYPTOLIB** algorithms for STM32



Why is FIPS important?

- Protection from unauthorized use
- Protection of critical security parameters
- Prevention of undetected modifications
- Use of approved security methods
- Indication of module operational status
- Detection and indication of errors

Who requires FIPS?

- All U.S. federal agencies
- Department of Defense (DOD)
- Financial institutions
- Postal authorities
- Adopted by the Canadian and UK Governments
- Private sector (encouraged but not required)

Thank you for your attention

/STM32

@ST_World

st.com/e2e

life.augmented

www.st.com/x-cube-cryptolib