Features

Supported NIST CAVP certified crypto algorithms:
- AES-128, AES-192, AES-256 bits:
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher-Block Chaining) with support for cipher text 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 cipher text stealing
- HASH functions with HMAC support:
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
- Random engine based on DRBG-AES-128
- RSA with PKCS#1v1.5:
  - Encryption/decryption
  - Signature
- ECC (Elliptic Curve Cryptography)
  - Key generation
  - Scalar multiplication (the base for ECDH)
  - ECDSA

Supported, but not certified, crypto algorithms included in the library:
- ARC4
- DES, TripleDES:
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher-Block Chaining)
- HASH:
  - MD5
  - HKDF-SHA-512
- ChaCha20
- Poly1305
- CChaCha20-Poly1305
- ED25519
- Curve25519
1 Description

The STM32 cryptographic library package (X-CUBE-CRYPTOLIB) includes all the major security algorithms for encryption, hashing, message authentication, and digital signing, enabling developers to satisfy application requirements for any combination of data integrity, confidentiality, identification/authentication, and nonrepudiation.

The library includes firmware as well as hardware-acceleration functions for STM32 families. For more details refer to STM32 crypto library User manual (UM1924) at the www.st.com website.

This firmware is classified ECCN 5D002.

Most of the well-used algorithms are certified according to the US Cryptographic Algorithm Validation Program (CAVP), helping customers to prove quickly and cost-effectively the security of their new products.

The certified algorithms are: AES (3971), RSA (2036), ECDSA (874), SHS (3275), DRBG (1165) and HMAC (2589). Full details are available online at the NIST CSRC Algorithm Validation Lists website http://csrc.nist.gov, selecting the Cryptographic Algorithm Validation Program web page.

In this package there are examples for each algorithm and template projects for popular development tools including Keil® MDK-ARM™, IAR® EWARM (IAR Embedded Workbench®) and GCC -based IDEs such as Ac6 SW4STM32 and Atollic® TrueSTUDIO®.

2 Ordering information

X-CUBE-CRYPTOLIB is available for free download from the www.st.com website.
3 Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-Sep-2015</td>
<td>1</td>
<td>Initial release.</td>
</tr>
<tr>
<td>09-Dec-2015</td>
<td>2</td>
<td>Updated <em>Features</em> and <em>Description</em> to introduce a new cryptographic firmware version.</td>
</tr>
<tr>
<td>15-Dec-2015</td>
<td>3</td>
<td>Updated <em>Description</em> and <em>Section 2: Ordering information</em>.</td>
</tr>
<tr>
<td>07-Jul-2016</td>
<td>4</td>
<td>Updated <em>Features</em> and <em>Description</em> to introduce the list of certified algorithms.</td>
</tr>
</tbody>
</table>
IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST's terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers' products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2016 STMicroelectronics – All rights reserved