HardCache™-SL3/PC v2.1 FIPS 140-2 Security Policy

HW Revision: STM7007

Contents

Introduction

The STMicroelectronics HardCache™-SL3/PC v2.1 Cryptographic Module (HW rev STM7007) is a single chip cryptographic module designed as a hardware accelerated encryption engine for computer and peripheral applications. The cryptographic module is targeted for PC applications including desktop client, laptop, and server systems. Benefits compared to competing hardware and software solutions include better overall system performance, low power, and tamper resistant hardware security. The cryptographic module is designed to be flexible, allowing administrative control of a wide range of features which simplify the security process to best fit an organization's requirements.

Cryptographic Boundary

The cryptographic boundary is defined as the outer perimeter of the single chip IC packaging, with 32 pins exposed as physical ports. The following image defines the cryptographic boundary:

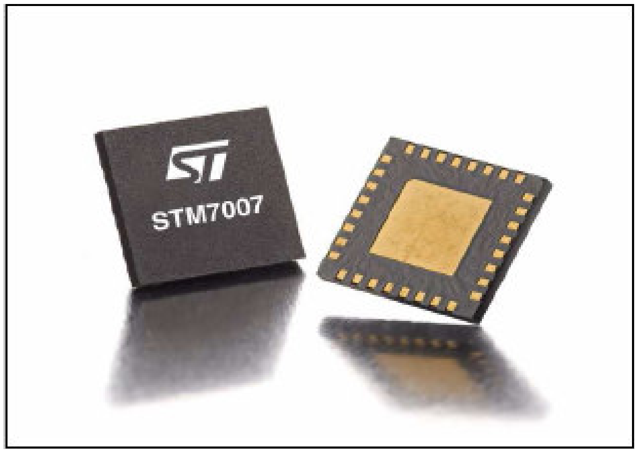

Figure 1 Specification of Cryptographic Boundary

Cryptographic Algorithms

The cryptographic module supports the following Approved cryptographic algorithms:

- AES 128, 192, 256 (ECB, CBC) Cert. #1068
- SHA-256, SHA-384, SHA-512 Cert. #1219
- HMAC-SHA-256, 384, 512 Cert. # 781
- TDES – 3keys (ECB, CBC) Cert. #798
- ECDSA Cert. #155
- RSA PKCS#1 v2.1, PSS ESMA (with SHA-256) Cert. #623
- ANSI X9.31 with AES-256 RNG Cert. #725

The cryptographic module supports the following non-Approved algorithms:
In firmware:

- RSA-2048 Decrypt PKCS#1 V2.1, OAEP (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- Non-approved hardware NDRNG (for seeding the Approved DRNG)

Physical Ports and Logical Interfaces

The cryptographic module support physical ports via 32 distinct pins, each with corresponding logical interfaces supported by the cryptographic module: data input, control input, data output, status output.

Table 1 ***Specification of Cryptographic Module Physical Ports and Logical Interfaces***

Physical Port	Logical Interface
Pin 1: REFCLK+	Control Input
Pin 2: REFCLK-	Control Input
Pin 3: 1.2V_PLL	Power
Pin 4: 1.2V TX	Power
Pin 5: PETp0	Data output, Status output
Pin 6: PETn0	Data output, Status output
Pin 7: 1.2V RX	Power
Pin 8: 2.5V	Power
Pin 9: PERn0	Data input, Control input
Pin 10: PERp0	Data input, Control input
Pin 11: 1.2V	Power
Pin 12: PP	Control Input
Pin 13: TDI	Control input
Pin 14: TRST#	Control input
Pin 15: PERST#	Control input
Pin 16: SS	Data output, Status output
Pin 17: 3.3V	Power
Pin 18: MOSI	Data output, Status output
Pin 19: MISO	Data input, Control input
Pin 20: SCLK	Data output, Status output
Pin 21: 2.5V	Power
Pin 22: rsvd	N/A – disabled
Pin 23: rsvd	N/A – disabled
Pin 24: CLKREQ#	Status output
Pin 25: PGOOD	Control Input
Pin 26: TDO	N/A - disabled
Pin 27: TCK	N/A - disabled
Pin 28: TMS	N/A - disabled
Pin 29: 1.2V	Power

Physical Port	Logical Interface
Pin 30: 2.5V PLL	Power
Pin 31: GND_PLL	Power
Pin 32: REFRES	Control Input

Security rules

The following specifies the security rules under which the cryptographic module shall operate:

- The cryptographic module provides a single mode of operation that is FIPS approved.
- Approved cryptographic algorithms shall be used to protect sensitive unclassified data. The cryptographic module shall not implement any Non-Approved cryptographic algorithms with the exception of RSA Decrypt for RSA based key transport and HW RNG for seeding the DRNG.
- The cryptographic module design shall correspond to its finite state model and design specifications.
- Critical security parameters shall be protected against unauthorized disclosure, modification and substitution. Public keys shall be protected against unauthorized modification and substitution.
- The cryptographic module shall not allow the input or output of plaintext critical security parameters.
- Logical separation between the data inputs, control inputs, data outputs, status outputs shall be enforced. The module shall receive power from an external source through its defined power ports.
- While in an error state, the cryptographic module shall inhibit all data outputs, cease to provide cryptographic services, and shall provide an error status indication (error code: GPE_SELF_TEST_FAILED or GPE_STARTUP_FAILED).
- All data outputs shall be inhibited during self-test conditions. Status information used to provide an indication of the results of self-tests shall not contain any CSPs, plaintext data, or other information that could be used to compromise the cryptographic module.
- All data output paths shall be logically disconnected from the processes performing key generation and zeroization.
- The cryptographic module shall not support manual key entry or split-knowledge processes.
- A maintenance interface and maintenance role shall not be supported.
- Cryptographic Officer, User and Storage Manager roles shall be supported.
- Identity-based authentication shall be enforced for all services that utilize CSPs, utilize Approved security functions, and are otherwise security relevant.
- Bypass capabilities, bypass states, and bypass tests shall not be supported.
- Service inputs shall consist of all data or control inputs to the module that initiate or obtain specific services, operations, or functions. Service outputs shall consist of all data and status outputs that result from the services, operations, or functions initiated or obtained by service inputs.

- The feedback mechanism used during the authentication process shall not disclose any CSP or other information that could be used to compromise the cryptographic module.
- Physical security provided by the cryptographic module via a hard enclosure that shall prevent penetration to the depth of the underlying circuitry without having a high probability that the module is damaged to the extent that it no longer functions. The cryptographic module shall be constructed of production grade materials with standard passivation, tamper evidence, and shall be opaque within the visible spectrum.
- The cryptographic module shall include a non-modifiable operational environment. It shall not be possible to physically or logically alter the executable instructions and logic that reside within the cryptographic boundary.
- Cryptographic keys shall be generated using the implemented Approved deterministic random number generator. The design shall ensure that the seed and seed key input to the Approved RNG do not have the same value. The key generation process shall provide an equivalent computational resistance to attack of at least 256-bits of security. Intermediate key generation values shall not be output from the cryptographic module during the key generation process.
- Seed keys and cryptographic keys shall be entered into and output from the cryptographic boundary in an encrypted form.
- A key-to-entity association shall be enforced for all keys that are entered into, output from, and stored within the cryptographic boundary.
- The implemented zeroization techniques shall be performed in a time that is not sufficient to compromise plaintext secret and private keys and CSPs.
- The cryptographic module shall conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).
- The cryptographic module shall support error states associated with each self-test and output the expected error indicator upon entering into an error state resulting from a failed self-test.
- The following self-tests shall be supported:

  Power up tests

  - Non-Approved hardware NDRNG continuous test
  - ANSI X9.31 with AES256 DRNG continuous test
  - HMAC-SHA-256 KAT
  - HMAC-SHA-512 KAT
  - AES 256 CBC encrypt/decrypt KAT
  - TDES 3 key CBC encrypt/decrypt KAT
  - RSA-2048 with SHA-256 signature generation/verification pairwise consistency test
  - ECDSA-256 signature generation KAT
  - ANSI X9.31 with AES256 DRNG KAT
  - HMAC-SHA-384 KAT
  - Critical functions test: RSA-2048 PKCS#1 V2.1, OAEP encrypt/decrypt pairwise consistency test

Conditional tests:

- Non-Approved hardware NDRNG continuous test
- ANSI X9.31 with AES256 DRNG continuous test
- RSA PKCS#1 V2.1, OAEP encrypt/decrypt pairwise consistency test

- Upon successful completion of the power-up self-tests, the cryptographic module shall output value 0 status; failure of any power-up self-test results in non-zero output status. The FIPS mode of operation indicator can be obtained through the "Get Capabilities" service which will return the following status: "fips140".
- An operator can initiate the power-up self-tests on demand via power cycle or via a command.

Identification and Authentication Policy

The cryptographic module supports a Cryptographic Officer and a User role through identity based authentication via HMAC verification using a 256-bit HMAC key. The cryptographic module also supports a Storage Manager role through identity based authentication via proof of possession of a 256-bit AES key through challenge/response.

Table 2 ***Roles and Required Identification and Authentication (FIPS 140-2 Table C1)***

Role	Type of Authentication	Authentication Data	Description
Cryptographic Officer	**Identity-based**	256-bit HMAC key (CO Session HMAC Key)	The cryptographic officer manages the cryptographic module and enrolls users/identities.
User	**Identity-based**	256-bit HMAC key (User Session HMAC Key)	Users load keys and execute cryptographic algorithms.
Storage Manager	**Identity-based**	256-bit AES key (Storage Manager AES Key)	Storage manager synchronizes the cryptomodule with the host system.

The strength of the implemented authentication mechanism exceeds the strength requirements imposed by FIPS 140-2. The following table declares the probabilities associated with random attempts, and multiple consecutive attempts within a one-minute period to subvert the implemented authentication mechanism.

Table 3 ***Strengths of Authentication Mechanisms (FIPS 140-2 Table C2)***

Authentication Mechanism	Strength of Mechanism

HMAC verification	The probability that a random attempt will succeed is 1 / 2^ 256. The probability of compromising the authentication mechanism through multiple consecutive attempt during a one minute period is 10000 / 2 ^ 256.
AES Challenge/Response	The probability that a random attempt will succeed is 1 / 2^ 256. The probability of compromising the authentication mechanism through multiple consecutive attempt during a one minute period is 10000 / 2 ^ 256.

Access Control Policy

The following table itemizes all of the roles, services, cryptographic keys & CSPs, and types of access to the cryptographic keys & CSPs that are available to each of the authorized roles via the corresponding services.

Definition of types of access:

I: input
O: output
G: generate
Z: zeroize
U: use

Table 4 ***Un-authenticated services***

Role	Services	Cryptographic Keys & CSPs	Type(s) of Access
None	Self Test	None	
None	Get Capabilities	None	
None	Get Status	None	
None	Zeroize cryptomodule	All CSPs are zeroized	Z

Table 5 *Services Authorized for Roles, Access Rights within Services (FIPS 140-2 Table C3, Table C4)*

Role			Services	Cryptographic Keys & CSPs	Type(s) of Access
C.O.	User	S.M.			
X			Initialize Cryptographic Module	EK Public Key EK Private Key CO AES Seed Key CO AES Nonce Key Storage Manager AES key AES Root Seed Key Random Number Pool ANSI X9.31 DT Seed ANSI X9.31 V Seed AES Root Key HMAC Root Key	G,I,O G,I,O,U I,O I,O I,O G,U G,U G,U G,U G,U G,U
X			Enroll Key	CO AES Seed Key CO AES Nonce Key CO Session AES Key CO Session HMAC Key User AES Seed Key AES Root Key HMAC Root Key	I,O,U I,O,U G,U G,U I,O U U
	X		Enter Key and Execute	User AES Seed Key User AES Nonce Key Data Key User Session AES Key User Session HMAC Key ANSI X9.31 DT Seed ANSI X9.31 V Seed AES Root Key HMAC Root Key	I,U I,U I,U G,U G,U G,I,O,U G,I,O,U U U
	X		Enter Key and Export	User AES Seed Key User AES Nonce Key Data Key User Session AES Key User Session HMAC Key ANSI X9.31 DT Seed ANSI X9.31 V Seed AES Root Key HMAC Root Key	I,O,U I,O,U I,O G,U G,U G,I,O,U G,I,O,U U U
		X	Authenticate Storage Manager	Storage Manager AES Key AES Root Key HMAC Root Key	I,U U U
		X	Flush context	User AES Seed Key User AES Nonce Key Data Key User Session AES Key User Session AES Key ANSI X9.31 DT Seed ANSI X9.31 V Seed	Z Z Z Z Z Z Z

		X	Save context	User AES Seed Key User AES Nonce Key Data Key User Session AES Key User Session AES Key ANSI X9.31 DT Seed ANSI X9.31 V Seed AES Root Key HMAC Root Key	O,Z O,Z O,Z G G G,I,O,U G,I,O,U U U
		X	Load context	User AES Seed Key User AES Nonce Key Data Key User Session AES Key User Session AES Key ANSI X9.31 DT Seed ANSI X9.31 V Seed AES Root Key HMAC Root Key	I I I I I I I U U

Description of the Services

- **Enter Key:** Cryptographic Officer seals (i.e. enrolls) a User key and User authentication data. The key and authentication data inserted into the module via AES key wrap transport scheme. The output key is available to a User for subsequent use.
- **Enter Key and Execute:** User loads his key into the cryptomodule in order to access services granted to both identity and the key kind; the following algorithms can be executed:
    - **AES:** User executes AES algorithm.
    - **TDES:** User executes TDES algorithm.
    - **HMAC:** User executes HMAC algorithm.
    - **SHS:** User executes Secure Hash Standard algorithm.
    - **RSA Sign:** User performs RSA PKCS#1 v2.1 PSS digital signature generation.
    - **ECDSA:** User executes ECDSA digital signature generation.
    - **Change Seed Keys:** User changes his own AES seed keys.
- **Enter Key and Export:** User exports his key using AES key wrap transport.
- **Authenticate Storage Manager:** Authenticates the Storage manager role.
- **Flush Key:** Storage manager zeroizes a key currently loaded in the cryptographic module.
- **Save Context:** Storage manager saves and zeroizes the key context currently loaded in the cryptographic module.
- **Load Context:** Storage manager loads a key for which context has been previously saved by the Storage Manager.

Unauthenticated Services

The following services do not disclose, modify, or substitute CSPs, use an Approved security function, or otherwise affect the security of the cryptographic module.

- **Self Test:** the cryptographic module performs all of the required power up self tests.
- **Get Capabilities:** gives information about the state of the device.
- **Get Status:** gives information about the state of non-security relevant hardware.
- **Zeroize:** zeroize all CSPs.

Physical Security Policy

The physical security employed by the cryptographic modules consists of a production grade IC packaging that is hard, opaque, and tamper evident. The following table described the responsibilities and actions required by the operator to ensure that physical security is maintained.

Table 6 *Inspection/Testing of Physical Security Mechanisms (FIPS 140-2 Table C5)*

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard, opaque, tamper evident IC packaging	Upon receipt	Perform a thorough visual inspection on all sides and angles of the enclosure for any signs of damage and malice including but not limited to scratches, scrapes, gouges, bent or broken pins, deterioration, discoloring. If any suspicious characteristics are observed, the cryptographic module is to be returned to the manufacturer.

Mitigation of Other Attacks Policy

Specify a security policy for mitigation of other attacks, including the security mechanisms implemented to mitigate the attacks.

Table 7 *Mitigation of Other Attacks (FIPS 140-2 Table C6)*

Other Attacks	Mitigation Mechanism	Specific Limitations
man-in-the-middle	session tracking with shared secret, rolling nonces, handle and signed messages	HMAC-SHA-256 integrity verification over authenticated services

replay	session tracking with shared secret, rolling nonces, handle and signed messages	HMAC-SHA-256 integrity verification over authenticated services

Achieved level of security

Table 8 *Achieved Level Of Security*

FIPS 140-2Security Requirements Area	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-tests	3
Design Assurance	3
Mitigation of Other Attacks	3

References

- [AES Key Wrap] National Institute of Standards and Technology (NIST), AES Key Wrap Specification, 2001 November
- [ANS X9.31 1998] American National Standard for Financial Services, Digital Signature Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
- [ANS X9.62 2005] American National Standard for Financial Services, Public Key Cryptography for the Financial Service Industry, ECDSA
- [FIPS140] National Institute of Standards and Technology (NIST), Security Requirements for Cryptographic Modules, FIPS Pub 140-2, 2001 May
- [FIPS 186] National Institute of Standards and Technology (NIST), Digital Signature Standard, FIPS Pub 186, 2006 March
- [NIST SP800-56] National Institute of Standards and Technology (NIST), Recommendation for Pair-Wise Key Establishment Scheme
- [NIST SP800-57] National Institute of Standards and Technology (NIST), Recommendation for Key Management – Part 1: General, NIST Special Publication 800-57, 2007 March
- [NIST SP800-90] National Institute of Standards and Technology (NIST), Recommendation for Random Number Generation Using Deterministic Random Bit Generators
- [NIST 931 RNG Ext] National Institute of Standards and Technology (NIST), Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using TDES and AES
- [PKCS#1 v2.1] RSA Laboratories, RSA Cryptography Standard