Intel® Offload and Crypto Subsystem (OCS)

HW version 4.0

FW version 4.0, 4.1, 4.2, 4.3

Document Version 1.5

Last updated: 2023-03-29

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

Table of Contents

1. Introduction *3*
1.1. Purpose Module Security Policy 3
1.2. Module Validation Level 3
2. Cryptographic Module Specification *4*
2.1. Module Overview 4
2.2. Module Components 5
2.3. Block Diagram 5
2.4. Modes of operation 6
2.4.1. FIPS-Approved cryptographic algorithms 6
3. Cryptographic Module Ports and Interfaces *8*
4. Roles, Services and Authentication *9*
4.1. Roles 9
4.2. Operator Authentication 9
4.3. Services 10
5. Physical Security *11*
6. Operational Environment *12*
7. Cryptographic Key Management *13*
7.1. Key Generation 13
7.2. Key Establishment/Key Derivation 13
7.3. Key Entry / Output 13
7.4. Key / CSP Storage 14
7.5. Key / CSP Zeroization 14
8. EMI/EMC *15*
9. Self-Tests *16*
9.1. Power-On Self-Tests 16
9.2. On-Demand Self-tests 16
9.3. Conditional Tests 16
10. Guidance *18*
10.1. Crypto Officer's Guidance 18
10.2. User's Guidance 18
10.3. Delivery Procedure 18
11. Mitigation of Other Attacks *19*
Appendix A. Glossary and Abbreviations *20*
Appendix B. References *21*

1. Introduction

This document is the non-proprietary FIPS 140-2 Security Policy for the Intel® Offload and Crypto Subsystem (OCS) cryptographic module (hereafter, “OCS”, “the module”, “OCS module”, “sub-chip module” are used interchangeably). This document contains a specification of the rules under which the module must operate and describes how it meets the requirements as specified in Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2) for a Security Level 2 hardware module. Itis intended for the FIPS 140-2 testing lab, Cryptographic Module Validation Program (CMVP), developers working on the release, administrators of the module and its users.

1.1. Purpose Module Security Policy

There are three major reasons that a security policy is required

- It is required for FIPS 140-2 validation.
- It allows individuals and organizations to determine whether the implemented Intel Offload and Crypto Subsystem satisfies the stated security policy.
- It allows individuals and organizations to determine whether the described capabilities, the level of protection, and access rights provided by the Intel Offload and Crypto Subsystem meet their security requirements.

1.2. Module Validation Level

The module is intended to meet requirements of FIPS 140-2 at an overall Security Level 2. Table 1 below shows the security level claimed for each of the eleven sections that comprise the FIPS 140-2 standard:

FIPS 140-2 Section		Security Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	2
Overall Level		2

Table 1: Security Levels

2. Cryptographic Module Specification

2.1. Module Overview

The Intel Offload and Crypto Subsystem is classified as a sub-chip hardware cryptographic module for FIPS 140-2 purposes. The cryptographic module is integrated in a single-chip module embodiment as defined in Section 4.5 of FIPS PUB 140-2.

The OCS is used to provide:

- Platform secure boot
- Runtime crypto acceleration
- Secured Global Secret Key storage

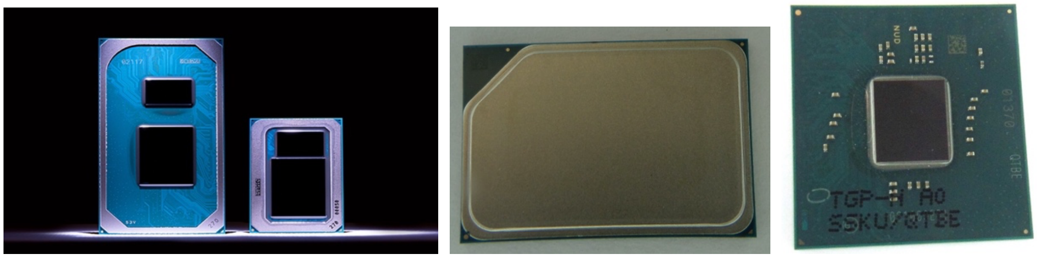

Figure 1: Test Platforms (Left to right: Tiger Lake-U, Elkhart Lake, and Tiger Lake -H/Rocket Lake-S[1])

The OCS is intended to be integrated onto an Intel platform and has been tested on the following:

Firmware Version	Hardware Version	Test Platform
4.0	4.0	Lakemont 3.7 embedded in Intel Tiger Lake-U with CSME OS running firmware version 15.0.20.1648.
4.1	4.0	Lakemont 3.7 embedded in Intel Rocket Lake-S with CSME OS running firmware version 15.0.22.1571.
4.2	4.0	Lakemont 3.7 embedded in Intel Tiger Lake -H with CSME OS running firmware version 15.0.30.1716.
4.3	4.0	Lakemont 3.7 embedded in Intel Elkhart Lake with CSME OS running firmware version 15.40.10.2204.

Table 2: Tested Platforms

[1] Intel Tiger Lake-H and Rocket Lake-S packages are identical

2.2. Module Components

The components that make up the sub-chip hardware cryptographic module are specified in Table 3:

Component	Type	Description
ECC	Hardware	Hardware crypto engines to offload ECDSA Digital Signatures Scheme.
AES	Hardware	Hardware crypto engines to offload a variety of AES operation modes.
HCU	Hardware	The Hash Control Unit implements a variety of hash functions.
SKS	Hardware	Secure Key Store for storing cryptographic keys used with cryptographic engines within the physical boundary.
RAM	Hardware	Reserved memory storage for OCS
OCS ROM	Firmware	Non-modifiable code which drives the hardware crypto engines and implements the operator authentication.

Table 3: Cryptographic Module Components

2.3. Block Diagram

The physical boundary of the OCS module is the single-chip physical boundary of the Test Platform listed in Table 2. The logical boundary of the module contains the OCS hardware engines, SRAM, and OCS ROM. The logical boundary is wholly contained within the physical boundary. There is exists no associated firmware that is externally loaded into the sub-chip cryptographic subsystem This is shown in Figure 2.

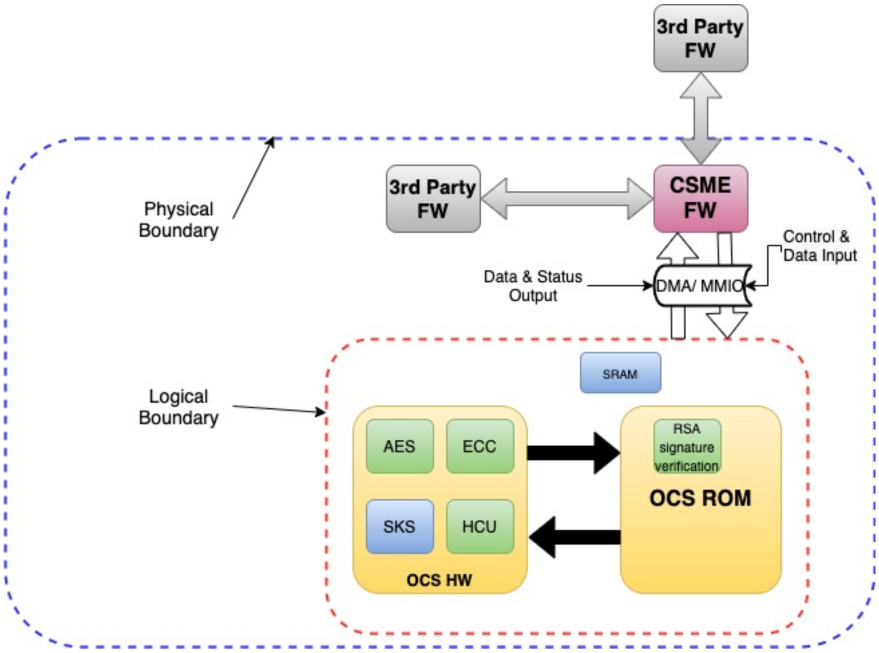

Figure 2: Block Diagram

2.4. Modes of operation

The module operates in one mode, the FIPS approved mode of operation. The module enters FIPS Approved mode after power-up tests succeed and the Operator Authentication has succeeded.

2.4.1. FIPS-Approved cryptographic algorithms

The module implements the following FIPS-Approved cryptographic algorithms:

Algorithm	Cryptographic Function	Standards	CAVP Certificates
AES Key Size: • 128-bit • 256-bit Modes: • ECB • CBC • CTR	Encryption decryption	FIPS 197, SP800-38A	A668
SHS • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512	Hashing	FIPS 180-4	A668
HMAC with: • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512	Message Authentication Code	FIPS 198-1	A668
ECDSA Curves: • P-256 • P-384 with: • SHA-224 • SHA-256 • SHA-384 • SHA-512	Digital Signature Generation and Verification	FIPS 186-4	A668

Table 4: FIPS-Approved Cryptographic Algorithms

Algorithm	Usage	Caveat
RSA Signature Verification[2] Modulo:3072 with SHA-384	User authentication purpose only.	(no security claimed) Allowed to be used in FIPS mode per IG 1.23

Table 4A: Non-approved Cryptographic Algorithm used in FIPS mode

[2] The algorithm has been tested with CAVP certificate #A668 but the known answer test has not been performed. RSA signature verification algorithm is only used as an authentication mechanism (see section 4.2 for details) and is not available as a service from the module. Therefore, the RSA algorithm does not share keys or CSPs used by any of the approved algorithm meeting the IG 1.23.

3. Cryptographic Module Ports and Interfaces

The physical input and output ports of this sub-chip module are MMIO (Memory-mapped I/O) and DMA (Direct Memory Access) where data is read (input) or written (output). The input and output is from the perspective of the sub-chip module under testing.

Physical ports are mapped to logical interfaces (i.e. module’s Application Programming Interface (API)) through which applications request services from the sub-chip module.

Table 5 summarizes the four logical interfaces and how they map to physical ports:

FIPS 140-2 Required Interfaces	Module Physical Ports	Module’s Logical interface
Data Input	MMIO registers, DMA	API’s input parameters
Data Output	MMIO registers, DMA	API’s output parameters
Control Input	MMIO registers	API functions calls
Status Output	MMIO registers	API’s return code
Power Input	Physical power port	N/A

Table 5: Ports and Interfaces

4. Roles, Services and Authentication

4.1. Roles

The module supports the following roles:

- **User role**: The application firmware (i.e. CSME FW shown in Figure 2) acting as a user utilizes all services provided by the module.
- **Crypto Officer (CO) role**: The CO is responsible for configuring the module in the FIPS Validated configuration as detailed in Section 10.1.

The module does not support concurrent operators.

4.2. Operator Authentication

The OCS module implements role-based authentication which requires that the module authenticates the authorization of an operator to explicitly assume a specific role and perform a corresponding set of services.

This module's authentication is based on RSA Signature Verification. The User (i.e. CSME FW) is signed by Intel. When the User FW is loaded onto the module a manifest file is appended to the image. The manifest file contains the FW image's public key and Signature. When the module is powered up, the OCS ROM authenticates the Operator by verifying the RSA signature using the provided public key. Upon successful signature verification, the module can begin providing services to the User. If the signature verification fails, the entire test platform (e.g. Intel Tiger Lake listed in Table 2) will enter the Error State until a hardware reset is performed. The module performs authentication upon every power cycle (e.g. power reset, power-off-to-power-on). The signing key (i.e. RSA private key) is controlled by Intel and is never shared to any external entities.

The Crypto Officer role is assumed only during when verifying the module's FIPS validated product status. The CO role does not require authentication since no cryptographic service that may affect the security of the module are performed by the CO.

Authentication type and data	Strength of Authentication (Single Attempt)	Strength of Authentication (Multiple-Attempt)
RSA Signature Verification	The public key used for authentication is RSA with bit length of 3072, yielding 128 bits of security strength. The chance of a random authentication attempt falsely succeeding is 1/(2^{128}) which is less than 1/1,000,000.	Considering a conservative rate of 1µs per failed authentication, which would allow 60,000,000 consecutive attempts per minute (60s / 0.001s), only provides a probability of successfully authenticating that is less than or equal to 60,000,000 * 1 / 2^{128} which is much less than 1 / 100,000

Table 6 Strength of Authentication

4.3. Services

The module provides services to users that assume one of the available roles upon their successful authentication. Table 7 details the Approved services and the non-Approved but allowed services in FIPS mode of operation, the roles that can request the service, the Critical Security Parameters involved and how they are accessed:

Service	Role	Key/CSP	Access
AES symmetric encryption and decryption	User	AES 128- and 256-bit keys	Read
ECDSA signature generation	User	ECDSA P-256 and P-384 public-private key pair	Read
ECDSA signature verification			Read
Message Digest generation (SHA-1/224/256/384/512)	User	None	None
Message Authentication Code generation and verification (HMAC SHA-1/224/256/384/512)	User	At least 112 bits HMAC key	Read
Show status	User	None	None
On-Demand Self-tests	User	None	None
SKS Key Storing (plaintext)	User	HMAC and AES keys, ECDSA public-private key pair	Write, Read
SKS Key Storing (encrypted)	User	AES Master Key, HMAC and AES keys, ECDSA public-private key pair	Write
Zeroization	User	All CSPs	Zeroize
Module Initialization	Crypto Officer	None	None

Table 7: Services available in FIPS mode of operation

5. Physical Security

The module is a defined as a hardware module implemented as a sub-chip and is identified as having a single-chip embodiment. The physical boundary is considered to be each platform listed in Table 2. The module conforms to the Security Level 2 requirements for physical security. The test platforms listed in Table 2 are commercial grade in regard to power and voltage ranges, temperature, reliability, and shock and vibration with industry standard passivation applied.

In addition, the module is covered with a tamper-evident coating that deters direct observation, probing, or manipulation of the single-chip.

6. Operational Environment

The module operates in a non-modifiable operational environment per FIPS 140-2 level 2 specifications and as such the operational environment requirements do not apply.

7. Cryptographic Key Management

Table 8 summarizes the Keys and Critical Security Parameters (CSPs) that are used by the cryptographic services implemented in the module:

Name	Generation / Entry	Storage	Zeroization
AES keys	The key is passed into the module via API input parameter. The key can also be loaded from the SKS directly to the register.	Stored as plaintext in the SRAM; Stored as plaintext or encrypted in SKS.	Keys stored in SRAM can be zeroized when power reset is performed; Keys stored in SKS can be zeroized when by setting cse_zeroing_en bit to '1' in control register.
HMAC keys	The key is passed into the module via API input parameter. The key can also be loaded from the SKS directly to the register.	Stored as plaintext in the SRAM ; Stored as plaintext or encrypted in SKS.	Keys stored in SRAM can be zeroized when power reset is performed; Keys stored in SKS can be zeroized when by setting cse_zeroing_en bit to '1' in control register.
ECDSA key pair	The ECDSA public-private keys are passed into the module via API input parameters. The key can also be loaded from the SKS directly to the register.	Stored as plaintext in the SRAM; Stored as plaintext or encrypted in SKS.	Keys stored in SRAM can be zeroized when power reset is performed; Keys stored in SKS can be zeroized when by setting cse_zeroing_en bit to '1' in control register.
AES master key	The key is passed into the module via API input parameters.	Stored as plaintext in the SKS	Zeroized by setting cse_zeroing_en bit to '1' in control register.

Table 8: Life cycle of Keys and Critical Security Parameters (CSP)

The following sections describe how CSPs, in particular cryptographic keys, are managed during its life cycle.

7.1. Key Generation

The module does not provide key generation functionality.

7.2. Key Establishment/Key Derivation

The OCS module does not perform any Key Establishment nor Key Derivation.

7.3. Key Entry / Output

The module does not support manual key entry or intermediate key generation key output.

All keys including symmetric AES keys and HMAC keys as well as asymmetric ECDSA key pairs are provided to the module via API input parameters. Additionally, the keys can be entered into in plaintext SKS for storage. The module does not produce key output in plaintext form outside its physical boundary.

7.4. Key / CSP Storage

The module provides Secure Key Storage (SKS). The keys stored in the SKS are in plaintext or encrypted with AES 256-bit master key. SKS is used to store keys in volatile memory only during runtime execution of the module. The keys stored in SKS are directly loaded into the register for ECDSA, AES or HMAC operations at the hardware level and cannot be retrieved by the calling application.

7.5. Key / CSP Zeroization

Keys passed into the module via API input parameters are zeroized from the memory by the OCS module before the API call returns to the calling application.

At the hardware level, two Memory-Mapped I/O (called “MMIO” in short) registers are used to store the keys temporarily: ECDSA_KEY, HCU_KEY and AES_KEY. These registers are write-only (i.e., user cannot read the keys from the registers) and they are mapped to the CSME Crypto Driver only (i.e., User Role; no other process is able to access these registers); therefore, the keys are protected by the hardware architecture before the key zeroization occurs. The keys are zeroized during the power-cycle of the module or by setting “cse_zeroing_en”. All other keys in the hardware components for the cryptographic operations are provided via the SKS which is wired hardware-internally to the cipher engines.

8. EMI/EMC

The OCS module cannot be certified by the FCC as it is not a standalone device. This module is a sub-chip embedded into one of the platforms listed in Table 2. The platforms listed there are also not standalone devices, but rather intended to be used within a COTS device which would undergo standard FCC certification for EMI/EMC.

According to 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, the Intel OCS is not subject to EMI/EMC regulations because it is a subassembly that is sold to an equipment manufacturer for further fabrication. That manufacturer is responsible for obtaining the necessary authorization for the equipment with the Intel OCS embedded prior to further marketing to a vendor or to a user.

9. Self-Tests

The module performs power-up self-tests and conditional tests to ensure the correctness of the cryptographic algorithm implementations within the module boundary. If any power-up self-test fails, the module halts in the Error state until a hardware reset is performed and the power-up self-test are rerun to recover from Error state. No data output and cryptographic operation are allowed in Error state.

9.1. Power-On Self-Tests

The module performs power-on self-tests tests automatically when the module is powered-on. The cryptographic algorithms are fully implemented in hardware, and as such, the integrity check is not applicable. Power-up tests only cover Known-Answer-Tests to ensure that all of the FIPS-Approved cryptographic algorithms work as expected. Table 9 below shows the power up self-tests supported by the OCS module.

Algorithm	Power-Up Tests
AES	• KAT AES-ECB Encryption • KAT AES-ECB Decryption
HMAC	• KAT HMAC-SHA-1 • KAT HMAC-SHA-256 • KAT HMAC-SHA-512
SHS	• KAT SHA-1 is covered in the KAT for HMAC-SHA-1 as allowed with IG 9.1 • KAT SHA-224 is not required per IG 9.4 • KAT SHA-256 is covered in the KAT for HMAC-SHA-256 is allowed with IG 9.1 • KAT SHA-384 is not required per IG 9.4 • KAT SHA-512 is covered in the KAT for HMAC-SHA-512 as allowed with IG 9.1
ECDSA	• KAT ECDSA (NIST P-256) signature generation • KAT ECDSA (NIST P-256) signature verification

Table 9: Self-Tests

For the KAT, the module calculates the result and compares it with the known value. If the answer does not match the known answer, the KAT is failed, and the module enters the Error state. While the module is executing the power-up tests, services are not available, and input and output are inhibited. The module does not return control to the calling application until the power-up tests are completed. Once the power-up tests are completed successfully, the module will be operational.

9.2. On-Demand Self-tests

The User Role can initiate On-Demand Self-tests by setting SELFTEST_RERUN control bit to trigger a reset which initiates the power-on self-tests. During the execution of the on-demand self-tests, services are not available, and no data output or input is possible.

9.3. Conditional Tests

The conditional tests do not apply to the OCS module because none of the conditions specified for the following tests occur:

- The module does not generate public or private keys. This test is not applicable.

- There is no software or firmware components of the module that are loaded into the module
- The module does not implement a random number generation service.
- The module does not support Bypass Mode.

10. Guidance

10.1.Crypto Officer’s Guidance

Upon first boot, the Crypto Officer shall query the module to determine whether it is a FIPS validated module by reading the “OCS_SELF_TEST_STATUS” register. Only if the module is a FIPS validated module will the Power-On Self-Tests run, and subsequently “OCS_SELF_TEST_STATUS.SELFTEST_PASS” bit will be set to 1. If the module is operational in a non FIPS validated module, this register will be set to 0.

10.2.User’s Guidance

There is no additional guidance for the User. Once the module has successfully completed the Self-Tests found in Section 9 and authenticated following guidance in Section 4.2, the module can begin providing Services listed in Section 4.3. The “Show Status” service can be called by reading the respective crypto engine status register (i.e. ECC_STATUS, HCU_STATUS, AES_STATUS, SKS_STATUS)

10.3.Delivery Procedure

The OCS module is contained within one of the platforms listed in Table 2. These Intel platforms are a tightly coupled component of 10th Generation Intel® Core™ chipsets. These platforms can be bundled with CPU as a kit, or outside the CPU packages as a discreet component mounted on the Printed Circuit Board (PCB). Intel requires their Original Equipment Manufacturer (OEM) partners that create, market, and sell these systems to meet the brand validation requirements and testing to ensure they have been designed and constructed with the proper components including CPU and Intel chipsets. Intel‘s brand validation tool would detect any mismatch of CPU and chipset for any system being designed.

Intel manages and implements security best practices throughout every step of their supply chain and works closely with their partners (i.e., Original Design Manufacturer and Original Equipment Manufacturer) to ensure that they meet Intel’s requirements for secure supply chain processes as specified in partner contract agreements.

11. Mitigation of Other Attacks

The OCS AES block cipher in OCS supports an implementation that is resistant to DPA (Differential Power Analysis attacks. The mechanism implemented is based on masking AES inputs at every stage with a pseudo-random mask. The seed for the pseudorandom mask generator is programmable.

The OCS ECC has protection against known Differential Power Attack (DPA) which is achieved by randomizing the inputs so there is no correlation to the power consumed and ECC operations. This is done by transforming inputs from one coordinate system (Affine) to another coordinate system (Randomized Jacobian).

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
API	Application Program Interface
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off The Shelf
CRNGT	Continuous Random Number Generator Test
CSE	Converged Security Engine
CSP	Critical Security Parameter
CTR	Counter Mode
DFx	Designed for X (manufacturability, testing and debugging). Primarily the debug interface for JTAG.
DMA	Direct Memory Access
EAU	Exponential Acceleration Unit
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standards Publication
HCU	Hash Control Unit.
HMAC	Hash Message Authentication Code
IG	Implementation Guidance
IME	Intel Management Engine (See ME below). Used on all PCH’s.
KAT	Known Answer Test
MAC	Message Authentication Code
ME	Management Engine
MMIO	Memory-Mapped I/O
NIST	National Institute of Science and Technology
OEM	Original Equipment Manufacturers
PCH	Platform Controller Hub
PCT	Pair-wise Consistency Test
PSS	Probabilistic Signature Scheme
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SKS	Secure Key Storage
SKU	Stock Keeping Unit

Appendix B. References

FIPS140-2 **FIPS PUB 140-2 - Security Requirements For Cryptographic Modules**
May 2001
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS140-2_IG **Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program**
November 5, 2021
https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips140-2/FIPS1402IG.pdf

FIPS180-4 **Secure Hash Standard (SHS)**
March 2012
http://csrc.nist.gov/publications/fips/fips180-4/fips 180-4.pdf

FIPS186-4 **Digital Signature Standard (DSS)**
July 2013
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

FIPS197 **Advanced Encryption Standard**
November 2001
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

FIPS198-1 **The Keyed Hash Message Authentication Code (HMAC)**
July 2008
http://csrc.nist.gov/publications/fips/fips198 1/FIPS-198 1_final.pdf

PKCS#1 **Public Key Cryptography Standards (PKCS) #1: RSA Cryptography**
Specifications Version 2.1
February 2003
http://www.ietf.org/rfc/rfc3447.txt

SP800-38A **NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques**
December 2001
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

SP800-131A **NIST Special Publication 800-131A - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths**
January 2011
http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf