High-level Summary of New/Updated Requirements Introduced with FIPS 140-3 (ISO/IEC 19790)

New Terminology Introduced	
Sensitive Security Parameters (SSP), which includes Critical Security Parameters (CSP) and Public Security Parameters (PSP)	
Differences that might require changes to the module/source code:	
Module Specification	
7.2.4.2 Approved service Indicator (New, All levels)	- All services shall provide an indicator when using an approved cryptographic algorithm, security function or process.
7.2.4.3 Degraded Mode of Operation **(New, All levels)**	- Optional support of a degraded operating mode (as a reconfiguration from the error state) in which the module will continue to support a subset of algorithms or services
Ports and Interfaces	
7.3.3 Control Output Interface **(New, All levels)**	- Commands to another cryptographic module can be sent through a newly defined control output interface. - Must be inhibited during both error state, and during any Self-Test
7.3.3 Unambiguous Input format **(New, All levels)**	- The module specification shall unambiguously specify the format of input data and control information, including length restrictions for all variable length inputs.
7.3.4 Trusted Channel **(Update, SL ≥ 3)**	- Requirement to implement a trusted channel (SL3,4) - Multi-Factor ID-based auth required for trusted channel (SL 4).
Roles, Services and Authentication	
7.4.3 Services **(New, All levels)**	- The module shall provide service to output module name/identifier and version that can be mapped to the validation records.
7.4.3.1 Services general Requirements (Update, All Levels)	- Zeroization of SSPs is now listed as a required service.
7.4.3.3 Self-Initiated Cryptographic Output Capability **(New, All levels)**	- Optional ability of the module to perform cryptographic operation without an operator request. - Two independent actions are required to activate this capability along with the status indicator.
7.4.3.4 Software/Firmware Loading **(Update, All levels)**	- Updated requirements when allowing loading of external software/firmware. For example, the module version shall be updated to reflect the loaded software/firmware.
7.4.4 Authentication **(Update, SL ≥ 2)**	- Explicit requirement to replace default authentication data after first-time authentication (SL 2,3,4) - Enforcement of authentication mechanism rules must be done by the module and not by procedure or documentation (SL2,3 4). - Requirement for multi-factor identity-based authentication (SL4). - The module shall implement an approved authentication mechanism as referenced in SP 800-140E (which points to SP800-63B). (All Levles). - Universal strength requirements for authentication has been updated to individual requirements for each approved authentication mechanism listed in SP 800-63B (All Levels).

Code Changes

Documentation Changes

Software/Firmware Security	
7.5 Software/Firmware Security **(Update, All levels)**	- Temporary values generated during Integrity test shall be zeroized. - On demand integrity test service is required. - There are additional requirements for the integrity test in relationship with software/firmware load test. - Software/firmware integrity test using approved hash algorithm, HMAC or digital signature (SL1) - Software/firmware integrity test using digital signature or HMAC (SL2) - The code of a CM shall only include code in executable form (SL2) - Software/firmware integrity test using digital signature only (SL3,4)
Operational Environment	
7.6 Operational Environment **(Update, SL2)**	- Module components are now explicitly stated as a minimum element of the Operational Environment in addition to the OS. - For modifiable operational environments, the audit mechanism has additional requirements and events that needs to be audited. Those are the following: - -- Use of a security relevant crypto officer function - -- requests to access auth data associated with the CM - -- the use of an auth mechanism associated with the CM - -- Explicit requests to assume a Crypto Officer role
Physical Security	
7.7.2 Physical Security General Requirements **(Update, SL ≥ 3)**	- Tamper evident seals shall be uniquely identified (SL3,4). - The module must include either EFP or EFT (SL3). - The module must include EFP and fault induction protection (SL4).
Non-invasive Security	
7.8 Non-invasive Security **(New, All levels)**	- Additional testing requirements for mitigation techniques (SL 3,4)
Sensitive security parameter management	
7.9 Sensitive Security Parameter Management **(Update, All levels)**	- Random Bit Generator (RBG) state information, hash values of passwords and intermediate key generation values are considered as CSPs.
7.9.2 Random Bit Generators **(Update, All levels)**	- If the entropy is collected outside of the module boundary, the data stream generated from this entropy input is considered a CSP.
7.9.5 Sensitive Security Parameter Entry and Output **(Update, All levels)**	- Electronic entry/output of CSPs, key components and authentication data via a wireless connection shall be in encrypted form. - Split knowledge procedures require a trusted channel (SL3,4). - Split knowledge procedures require multi-factor authentication (SL4).
7.9.7 Sensitive Security Parameter Zeroization **(New, All levels)**	- Zeroization is required for all unprotected SSP (not just CSPs). - Zeroization of unprotected SSPs may be done procedurally (SL1). - Status indicator is required when zeroization is complete (SL 2,3,4). - Zeroization of all (protected and unprotected) SSPs shall return the module to its factory state (SL4).
Self-Tests	
7.10 Self-tests **(Update, All levels)** **(New, SL ≥ 3)**	- No data or control output shall be allowed via control or data output interface when the module is in the error state. - If a CM does not output an error status after failing a test, the operator of the module shall be able to determine if the module has entered an error state implicitly through an unambiguous procedure documented in the SP. - New requirement to maintain error log of most recent error (SL3,4)

Code Changes

Documentation Changes

7.10.2 Pre-operational Self-tests **(Update, All levels)**	- Consist of software/firmware integrity, bypass (if applicable) and critical function test (if applicable) - Algorithm self-tests have been moved from power-up test to conditional test phase (prior to first use of algorithm) with exception of 1. Algorithm used for integrity test needs to be tested with self-test. 2. Hardware modules with no software/firmware need to implement at a minimum one algorithm self-test. - Power-up bypass self-test required in addition to the conditional test.
7.10.3 Conditional Self-tests **(Update, All levels)**	- Algorithm will be self-tested during conditional test, before first use. - Algorithm self-tests (section 7.10.3.2) do not include a Pairwise-Consistency Test (PCT). ISO/IEC 19790 does not permit a PCT be conducted in lieu of a KAT, as allowed in FIPS 140-2 DTR (AS09.18). - Introduction of Fault-detection test as an algorithm self-test - Manual entry test (if applicable) shall be performed for SSPs (not just CSPs).
7.10.3.6 Conditional Bypass test **(Update, All levels)**	- If the module maintains internal information governing the bypass capability, then this information shall be protected with an approved integrity technique - Any modification to the governing information requires recalculating the integrity value.
7.10.3.8 Periodic Self-tests **(Update, SL ≥ 3)**	- The module must perform periodic execution of self-tests automatically without requiring any external input (SL3,4). - The time-period and conditions that may result in interrruption of operation during self-tests shall be specified in the SP (SL3,4)
Design	
7.11.3 Design **(New, All levels)**	- Cryptographic modules design must allow the testing of all security related services provided by the module.
7.11.4 Finite State Model **(Update, All levels)**	- Addition of “General Initialization state" and “Approved State” and optional “Quiescent state” indicating that the module is dormant. - Entering Crypto Officer state from any other role is not allowed. - Addition of new elements to the FSM description such as “degraded operation”, “control output interface” and “trusted channel”
Differences that might require changes to the documentation:	
Module Specification	
7.2.4.3 Degraded Mode of Operation **(New, All levels)**	- Optional degraded operating mode in which the module will support a subset of algorithms/services when the module exits out of an error state.
Roles, Services and Authentication	
7.4.2 Roles **(Update, All levels)**	- The module must support a Crypto Officer role at a minimum. The User role is no longer a required role.
Non-invasive Security	
7.8 Non-invasive Security **(New, All levels)**	- The documentation shall specify any implemented mitigation technique (referenced in 140F) for non-invasive attacks.
Configuration Management	
7.11.2 Configuration Management (CM) **(Update, All levels)**	- There is an explicit requirement for the CM system to track each configuration item revision throughout the module life-cycle. - The CM system has to be automated (SL3,4).
7.11.5 Development **(Update, All levels)**	- For hardware modules, HDL shall be annotated with comments. - For software, firmware, and hybrid modules:

Code Changes

Documentation Changes

	1. Resources used to form the executable shall for be tracked by CM. 2. Documentation shall list the compiler & configuration options used. 3. Result of integrity & authentication technique shall be integrated in the module. 4. Production-grade development tools shall be used. - All software, firmware and HDL shall be designed with high level languages, or a rationale is required for the use of a low-level language (SL2,3,4). (FIPS 140-2 required this only for Level 3 and 4.) - The requirement for a formal model at SL4 no longer exists.
7.11.6 Vendor Testing **(New, All levels)**	- The documentation shall specify vendor's functional testing. - The use of automated security diagnostic tools is required for software, firmware and hybrid modules. - Requirement to document vendor's low-level module testing (SL3,4)
7.11.7 Delivery and Operation **(Update, SL ≥ 2)**	- The documentation shall include procedures for tamper detection during delivery (SL2,3,4). - The authorized operator is required to be authenticated (SL4).
7.11.8 End of Life **(New, All levels)**	- The documentation must specify procedures for secure sanitization of the module (SL1,2). - The documentation must specify procedures for secure destruction of the module (SL3,4).
7.11.8 Guidance **(Update, All levels)**	- The administrator guidance shall state the procedures required to keep authentication data and the mechanism independent.
Mitigation of other Attacks	
7.12 Mitigation of other Attacks (**Update, SL4**)	- Documentation of the methods used to test the effectiveness of the mitigation techniques is required (SL4).
Cryptographic Module Security Policy	
14 B - Cryptographic Module Security Policy	- The Security Policy must include everything listed in Annex B.2 in the specified order.

Code Changes

Documentation Changes

FIPS 140-3

	Security Level 1			Security Level 2			Security Level 3			Security Level 4		
	AS	VE	TE	AS	VE	TE	AS	VE	TE	AS	VE	TE
Section 01	4	0	0	4	0	0	4	0	0	4	0	0
Section 02	32	40	65	32	40	65	32	40	65	32	40	65
Section 03	13	32	42	13	32	42	19	40	51	20	41	52
Section 04	38	36	45	52	47	63	55	48	70	56	49	71
Section 05	13	16	30	18	19	37	23	21	39	23	21	39
Section 06	8	5	10	28	24	50	0	0	0	0	0	0
Section 07	18	9	14	32	19	27	62	39	68	76	47	77
Section 08	5	3	3	5	3	3	6	4	4	6	4	4
Section 09	24	26	44	28	29	48	31	32	55	34	32	57
Section 10	51	41	68	51	41	68	55	46	74	55	46	74
Section 11	26	26	38	33	32	44	36	35	47	39	40	52
Section 12	2	2	2	2	2	2	2	2	2	4	5	5
Section A	1	1	1	1	1	1	1	1	1	1	1	1
Section B	3	4	4	3	4	4	3	4	4	3	4	4
Total	238	241	366	302	293	454	329	312	480	353	330	501
% Increase	**27.3**	**40.1**	**39.2**	**39.2**	**52.6**	**50.8**	**32.1**	**42.5**	**30.8**	**24.3**	**40.4**	**28.8**

FIPS 140-2

	Security Level 1			Security Level 2			Security Level 3			Security Level 4		
	AS	VE	TE	AS	VE	TE	AS	VE	TE	AS	VE	TE
Section 01	15	24	29	15	24	29	16	26	31	16	26	31
Section 02	15	22	33	15	22	33	18	25	38	18	25	38
Section 03	19	18	28	28	22	38	28	22	39	28	22	39
Section 04	5	1	12	5	1	12	5	1	12	5	1	12
Section 05	18	12	16	28	20	25	41	29	56	68	38	71
Section 06	8	6	7	16	11	23	20	15	32	20	15	32
Section 07	35	24	47	35	24	47	42	29	59	42	29	59
Section 08	4	3	4	4	3	4	4	3	4	4	3	4
Section 09	46	37	66	46	37	66	47	39	70	48	40	72
Section 10	12	12	12	15	15	15	18	17	17	25	23	22
Section 11	1	2	2	1	2	2	1	2	2	1	2	2
Section 14	9	11	7	9	11	7	9	11	7	9	11	7
Total	187	172	263	217	192	301	249	219	367	284	235	389