# List of Documentation needed for FIPS 140-2

The following is a list of documentation that is needed for successful testing of a cryptographic module. Although atsec do not require the documentation to be in the exact format and documents specified, we **DO** need to have all the information required. We do not specify which format the information is presented to us.

This and other information is also available in FIPS 140-2 Appendix "A"

### *CRYPTOGRAPHIC MODULE SPECIFICATION*

- Specification of the hardware, software, and firmware components of a cryptographic module, specification of the cryptographic boundary surrounding these components, and description of the physical configuration of the module. *(Security Levels 1, 2, 3, and 4)*
- Specification of any hardware, software, or firmware components of a cryptographic module that are excluded from the security requirements of this standard and an explanation of the rationale for the exclusion. *(Security Levels 1, 2, 3, and 4)*
- Specification of the physical ports and logical interfaces of a cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- Specification of the manual or logical controls of a cryptographic module, physical or logical status indicators, and applicable physical, logical, and electrical characteristics. *(Security Levels 1, 2, 3, and 4)*
- List of all security functions, both Approved and non-Approved, that are employed by a cryptographic module and specification of all modes of operation, both Approved and non-Approved. *(Security Levels 1, 2, 3, and 4)*
- Block diagram depicting all of the major hardware components of a cryptographic module and component interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory. *(Security Levels 1, 2, 3, and 4)*
- Specification of the design of the hardware, software, and firmware components of a cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- Specification of all security-related information, including secret and private cryptographic keys (both plaintext and encrypted), authentication data (e.g., passwords, PINs), CSPs, and other protected information (e.g., audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module.
- Specification of a cryptographic module security policy including the rules derived from the requirements of this standard and the rules derived from any additional requirements imposed by the vendor). *(Security Levels 1, 2, 3, and 4)*

### *CRYPTOGRAPHIC MODULE PORTS AND INTERFACES*

- Specification of the physical ports and logical interfaces of a cryptographic module and all defined input and output data paths. (Security Levels 1, 2, 3, and 4)

### *ROLES, SERVICES, AND AUTHENTICATION*

- Specification of all authorized roles supported by a cryptographic module. (Security Levels 1, 2, 3, and 4)
- Specification of the services, operations, or functions provided by a cryptographic module, both Approved and non-Approved. For each service, specification of the service inputs, corresponding service outputs, and the authorized role(s) in which the service can be performed. (Security Levels 1, 2, 3, and 4)
- Specification of any services provided by a cryptographic module for which the operator is not required to assume an authorized role, and how these services do not modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the module.

- Specification of the authentication mechanisms supported by a cryptographic module, the types of authentication data required to implement supported authentication mechanisms, the authorized methods used to control access to the module for the first time and initialize the authentication mechanism, and the corresponding strength of the mechanisms supported by the module. (Security Levels 2, 3, and 4)

***FINITE STATE MODEL***

- Representation of a finite state model (or equivalent) using the state transition diagram and/or state transition table that specifies all operational and error states, corresponding transitions from one state to another, input events (including data inputs and control outputs) that cause transitions from one state to another, and output events (including internal module conditions, data outputs, and status outputs) resulting from transitions from one state to another. (Security Levels 1, 2, 3, and 4)

**PHYSICAL SECURITY**

- Specification of the physical embodiment and security level for which the physical security mechanisms of a cryptographic module are implemented. Specification of the physical security mechanisms that are employed by a module. (Security Levels 1, 2, 3, and 4)
- If a cryptographic module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access, specification of the maintenance access interface and how plaintext secret and private keys and CSPs are to be zeroized when the maintenance access interface is accessed. (Security Levels 1, 2, 3, and 4)
- Specification of the normal operating ranges of a cryptographic module. Specification of the environmental failure protection features employed by a cryptographic module or specification of the environmental failure tests performed. (Security Level 4)

**OPERATIONAL ENVIRONMENT**

- Specification of the operational environment for the cryptographic module. (Security Levels 1, 2, 3, and 4)
- Identification of the operating system employed by a cryptographic module, the applicable Protection Profile, and the CC assurance level. (Security Levels 2, 3, and 4)

**CRYPTOGRAPHIC KEY MANAGEMENT**

- Specification of all cryptographic keys, cryptographic key components, and CSPs employed by a cryptographic module.
- Specification of each RNG (Approved and non-Approved) employed by a cryptographic module. (Security Levels 1, 2, 3, and 4)
- Specification of each of the key generation methods (Approved and non-Approved) employed by a cryptographic module. (Security Levels 1, 2, 3, and 4)
- Specification of the key establishment methods employed by a cryptographic module. (Security Levels 1, 2, 3, and 4)
- Specification of the key entry and output methods employed by a cryptographic module. (Security Levels 1, 2, 3, and 4)
- If split knowledge procedures are used, proof that if knowledge of n key components is required to reconstruct the original key, then knowledge that any n-1 key components provides no information about the original key other than length, and specification of the split-knowledge procedures employed by a cryptographic module. (Security Levels 3 and 4)

- Specification of the key storage methods employed by a cryptographic module. (Security Levels 1, 2, 3, and 4)
- Specification of the key zeroization methods employed by a cryptographic module. (Security Levels 1, 2, 3, and 4)

**ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY •**

- Proof of conformance to EMI/EMC requirements. (Security Levels 1, 2, 3, and 4)

**SELF-TESTS**

- Specification of the self-tests performed by a cryptographic module including power-up and conditional tests. (Security Levels 1, 2, 3, and 4)
- Specification of the error states that a cryptographic module can enter when a self-test fails, and the conditions and actions necessary to exit the error states and resume normal operation of a module. (Security Levels 1, 2, 3, and 4)
- Specification of all security functions critical to the secure operation of a cryptographic module and identification of the applicable power-up tests and conditional tests performed by the module. (Security Levels 1, 2, 3, and 4)
- If a cryptographic module implements a bypass capability, specification of the mechanism or logic governing the switching procedure. (Security Levels 1, 2, 3, and 4)

**DESIGN ASSURANCE**

- Specification of procedures for secure installation, generation, and start-up of a cryptographic module. (Security Levels 1, 2, 3, and 4)
- Specification of the procedures for maintaining security while distributing and delivering versions of a cryptographic module to authorized operators. (Security Level 2, 3, and 4)
- Specification of the correspondence between the design of the hardware, software, and firmware components of a cryptographic module and the cryptographic module security policy (i.e., the rules of operation). (Security Levels 1, 2, 3, and 4)
- If a cryptographic module contains software or firmware components, specification of the source code for the software and firmware components, annotated with comments that clearly depict the correspondence of the components to the design of the module. (Security Levels 1, 2, 3, and 4)
- If a cryptographic module contains hardware components, specification of the schematics and/or Hardware Description Language (HDL) listings for the hardware components. (Security Levels 1, 2, 3, and 4)
- Functional specification that informally describes a cryptographic module, the external ports and interfaces of the module, and the purpose of the interfaces. (Security Levels 2, 3, and 4)
- Specification of a formal model that describes the rules and characteristics of the cryptographic module security policy, using a formal specification language that is a rigorous notation based on established mathematics, such as first order logic or set theory. (Security Level 4)
- Specification of a rationale that demonstrates the consistency and completeness of the formal model with respect to the cryptographic module security policy. (Security Level 4)
- Specification of an informal proof of the correspondence between the formal model and the functional specification. (Security Level 4)
- For each hardware, software, and firmware component, source code annotation with comments that specify (1) the preconditions required upon entry into the module component, function or procedure in order to execute correctly and (2) the postconditions expected to be true when execution of the module component, function, or procedure is complete. (Security Level 4)

- Specification of an informal proof of the correspondence between the design of the cryptographic module (as reflected by the precondition and postcondition annotations) and the functional specification. (Security Level 4)
- For crypto officer guidance, specification of:
    - assumptions regarding user behavior that is relevant to the secure operation of the cryptographic module. *(Security Levels 1, 2, 3, and 4)*
- For user guidance, specification of
    - the Approved security functions, physical ports, and logical interfaces available to the users of the cryptographic module (Security Levels 1, 2, 3, and 4), and
    - all user responsibilities necessary for the secure operation of the module. (Security Levels 1, 2, 3, and 4)

**MITIGATION OF OTHER ATTACKS**

- If a cryptographic module is designed to mitigate one or more specific attacks, specification in the module's security policy of the security mechanisms employed by the cryptographic module to mitigate the attack(s). (Security Levels 1, 2, 3, and 4)

***SECURITY POLICY***

- See Appendix C of FIPS 140-2. (Security Levels 1, 2, 3, and 4)