Understanding

FIPS 140-2 SINGLE-CHIP LEVEL 3 PHYSICAL SECURITY

BY TRAVIS SPANN AND THE AEGISOLVE TEAM

VERSION 1.0 | JULY 2018

ÆGISOLVE

Project Background and Description

The purpose of this document is to provide an overview of the FIPS 140-2, Security Requirements for Cryptographic Modules requirements as they relate to Level 3 single-chip physical security.

Overall Requirements

The FIPS 140-2 identifies and addresses three physical embodiments for cryptographic modules:

1. Single-chip (a single IC).
2. Multi-chip embedded (Two or more interconnected ICs embedded within an enclosure or product that may itself not be physically protected).
3. Multi-chip standalone (Two or more interconnected ICs embedded within a physically protected standalone enclosure).

Additionally, the FIPS 140-2 specifies four Security Levels (1-4) with the following physical security requirements for single-chip modules:

- Level 1: Production grade components.
- Level 2: The IC must be encapsulated within an opaque coating which provides tamper evidence.
- Level 3: The IC must be encapsulated within a hard, opaque, tamper-evident coating or a strong removal-resistant and penetration resistant enclosure.
- Level 4: N/A for this report.

VERSION 1.0 | JULY 2018

ÆGISOLVE

Level 3 Single-chip Requirements

So we see from above that the following requirements apply to level 3 single-chip modules:

- **Production grade components including standard passivation, reliability, data sheets, etc.**
- **Tamper Evidence:** The FIPS testing laboratory will verify that attempts to enter or probe the single-chip module will result in scratches or markings on the exterior surface of the IC.
- **Opacity:** Most ICs come in one of two embodiments, a bare die with bonding pads visible along some, or all, sides of the die. In this case the lab will verify that no circuitry configuration is visible that might help an attacker to determine where to probe the IC to possibly discover any module Critical Security Parameters (CSPs), such as secret or private keys or PINs. Please note that the FIPS testing laboratory does not have to actually probe and read any module CSPs, they merely have to conclude that reading module CSPs is possible with the appropriate equipment. The second embodiment is where an IC vendor will encapsulate the individual IC die with a plastic or other hard material to allow easier assembly of the IC onto a printed circuit board. In this case the testing laboratory will verify that the IC encapsulation is hard, and opaque within the visible light spectrum.

  The Cryptographic Module Validation Program (CMVP) at NIST has released guidance relevant to opacity testing:

  - NIST's Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program document, Implementation Guidance IG 5.1 entitled 'Opacity and Probing of Cryptographic Modules with Fans, Ventilation Holes or Slits at Level 2' states, "The purpose of the opacity requirement is to deter direct observation of the cryptographic module's internal components and design information to prevent a determination of the composition or implementation of the module."
  - **From the same document, IG 5.3 entitled, 'Physical Security Assumptions' states the following requirements relevant to level 3 Single-chip modules:**
    - Observable evidence of tampering
    - Physical boundary of the chip is opaque to prevent direct observation of internal security components, e.g., the die is encapsulated with an opaque material
    - Direct entry/probing attacks prevented, e.g., the die is encapsulated.
    - Strong tamper resistant encapsulation material

(...continued on next page)

Level 3 Single-chip Requirements (continued)

- **Hardness:** The FIPS 140-2 Derived Test Requirements, in AS.05.28 and AS.05.29, specifies the following two hardness requirements for single-chip modules thusly:
    - AS.05.28 states, "Single-chip: Levels 3 and 4: Either the cryptographic module shall be covered with a hard-opaque tamper-evident coating (e.g., a hard-opaque epoxy covering the passivation or AS05.29 shall be satisfied."
    - AS.05.29 states, "Single-chip: Levels 3 and 4: Either the enclosure shall be designed so that attempts at removal or penetration of the enclosure shall have a high probability of causing serious damage to the cryptographic module (i.e., the module will not function) or AS.05.28 shall be satisfied.
    - NIST further defines the hardness requirements in their FIPS 140-2 Implementation Guidance IG 5.4 Level 3: Hard Coating Test Methods. The key points being:
        - **Hard/hardness definition:** "The relative resistance of a metal or other material to denting, scratching, or bending; physically toughened; rugged, and durable. The relative resistances of the material to be penetrated by another object."
        - **Test methods** shall be consistent with a "moderately aggressive attack".
        - **The test methods shall at a minimum address the hardness characteristics of the epoxy or potting material as follows:**
            1. Attempts to penetrate the material by an instrument (e.g. awl, pointed handheld tool, etc.) using moderately aggressive amount of force to the depth of the underlying circuitry. The use of a drilling or grinding motion is out-of-scope.
            2. The use of an instrument with a moderately aggressive amount of force to pry or break the material away from the underlying circuitry (e.g. insert a pry instrument at the boundary of the epoxy or potting material and another material/component (e.g. PCB board).
            3. The use of a moderately aggressive amount of flexing or bending force to crack or break the material away from or expose the underlying circuitry.
        - During testing the module should be consistently assessed to determine if serious damage has occurred (i.e. the module will either cease to function or the module is unable to function).
        - Hardness testing is performed throughout the specified nominal operating temperature range.

Major Takeaways

Important implications of the FIPS 140-2 single-chip Level 3 physical security requirements.

ROBUST REQUIREMENTS

- FIPS 140-2 Security Level 3 single-chip devices are robust and relevant for many industries including, but not limited to, IoT, automotive, banking, healthcare and digital cinema.

DEVELOPER GUIDANCE

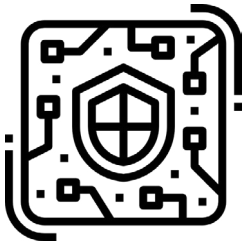
- Understanding the applicable test requirements enables product developers to make better implementation decisions.

SMART CHIPS, SLOW CHIPS

- It is important to keep in mind that when choosing the single-chip module that will meet higher level physical security requirements, smart card chips might seem a good choice. The fact that they have a relatively slow throughput, however, might remove them from consideration in some multi-chip system architectures.

CONSUMER GUIDANCE

- Knowing what standards are in place for the latest hardware, consumers and businesses are better equipped to make product selections in the open market.



Need Help Understanding How Level 3 Single-Chip physical Security Impacts Your Business? **We can help.**

aegisolve.com/fips-sc3-request

VERSION 1.0 | JULY 2018

ÆGISOLVE

REFERENCES

- *FIPS PUB 140-2 Security Requirements for Cryptographic Modules*
- *Derived Test Requirements for FIPS PUB 140-2 Security Requirements for Cryptographic Modules*
- *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program*

About AEGISOLVE

AEGISOLVE is the industry leader in providing Federal Information Processing Standards (FIPS 140-2) testing and validation certificates (NVLAP Lab Code: 200802-0). As an all-in-one solution, Aegisolve is the world's first and only single-source-supplier for Digital Cinema Initiatives CTP validations.

AEGISOLVE.COM

(650) 386-1436

415 Fairchild Dr, Mountain View, CA 94043

VERSION 1.0 | JULY 2018

ÆGISOLVE