IGs 7.18, 7.19 and the Draft IG 7.20

Alex Calis

Allen Roginsky

April 27, 2021

The Entropy IGs

- The relevant FIPS 140-2 IGs:
  - 7.14, 7.18, 7.19 and 7.20 (to be published soon)
- The FIPS 140-3 versions – later in the presentation

- IG 7.14 shows when entropy estimation is required
- IG 7.18 governs the transition
- IG 7.19 provides some useful tools for meeting the SP 800-90B requirements
- IG 7.20 anticipates the publication of SP 800-90C and provides the vendor with certain options to use before SP 800-90C becomes available
- A word about IG 7.15

Very Important

These IGs do not introduce any new requirements. The shall statements found in these IGs are the interpretations of the shall statements in SP 800-90B.

Some SP 800-90B requirements (and the future SP 800-90C requirements) have been made less strict by the IGs

When Do Entropy Estimation Requirements Apply?

- When the module is either generating the entropy itself or making a call to request the entropy from a well-defined source
  - A hardware module with an entropy source inside the module's cryptographic boundary
  - A software module making a call to a source within the module's physical boundary
- It is slightly more complicated when a hybrid approach is used but the idea is the same. The entropy testing requirement only applies to the actively generated / received entropy.
- This is IG 7.14. SP 800-90C will show some additional cases.

When Do Entropy Estimation Requirements NOT Apply?

- When the entropy is obtained passively and/or there is no control over the amount of passed entropy
  - An entropy input is generated outside the module's physical boundary (by another module or the manufacturer)
  - A software module that receives an unsolicited Load command (even if from an entropy source located inside the module's physical boundary)

- An appropriate caveat shall appear in the module's validation certificate

IG 7.18 – Transitioning to SP 800-90B

- If a Test Report is submitted today and IG 7.14 indicates that entropy estimation shall be performed, then the entropy source shall comply with SP 800-90B.
- Vendors shall provide the testing laboratory with access to raw data
- The CST lab shall submit an Entropy Test report demonstrating the source's compliance with SP 800-90B
- NIST has made a statistical testing tool available

IG 7.18 – Continued

- The approved algorithms used in the vetted conditioning components shall be tested by the CAVP. The self-tests for these algorithms are optional if the algorithm's implementation is not otherwise used by the module.
- The stationary behavior of the noise source (section 3.2.2 of SP 800-90B) does not have to be demonstrated
- Special attention to an IID claim. The heuristic proofs of both the independence and the identical distribution are required

- IG 7.15 does not apply but some of its suggestions can be useful when performing a heuristic analysis of entropy

IG 7.19 - Interpretation of SP 800-90B Requirements

- 18 resolutions and 5 Additional Comments – all to make designing, testing and validating entropy sources easier
- A Conditioning Chain is introduced
- Simplified testing requirements for the bijective conditioning components – no statistical testing for such non-vetted conditioning components
- The permission for the conditioning component to retain the state between invocations

IG 7.19 - Continued

- Multiple ring oscillators may be treated as copies even if their design and parameters may vary
- A reminder that the health tests shall be tailored to detect the likely failures of a specific noise source
- The suggestions for how to use the simulation to meet the Section 4.5 of SP 800-90B requirements for the developer-defined health tests
- A requirement to perform the verification of the correct implementation of each conditioning component

IG 7.20 - Combining Entropy from Multiple Sources

Question:

Why bother until SP 800-90C is published?

IG 7.20 - Continued

Answer:

- A confusion among the vendors and the testing labs about combining any sources, given that SP 800-90B does not allow adding the entropies obtained from the (somewhat different) noise sources
- It is clear that SP 800-90C will allow concatenating entropy bitstrings from multiple independent entropy sources
- The need to specify in the validation certificate if only physical sources are used. The ENT(P) and ENT(NP) notation.

More on IG 7.20

The Limitations:

- An external conditioning will be allowed in SP 800-90C. Not in IG 7.20.
- The only way the multiple entropy sources may be combined is by concatenating their output bitstrings
- If an independence of the entropy sources is not established, then only one entropy source can be credited

Questions?

CMVP: cmvp@nist.gov & CMVP@cyber.gc.ca

Alex Calis: alexander.calis@nist.gov

Allen Roginsky: allen.roginsky@nist.gov.