FIPS140-3 Overview: 90-B Validations

National Institute of Standards and Technology
U.S. Department of Commerce

Tim Hall, NIST

Chris Celi, NIST

SP800-90B Entropy Validation Timeline

- January 2018 – SP800-90B published
- Summer 2020 – Entropy Source Validation Test System (ESVTS) development begins
- June 30, 2020 – CAVS Tool retired; algorithm validations performed through Automated Cryptographic Validation Test System (ACVTS)
- November 7, 2020 – SP800-90B requirements must be met for 140-2 modules according to IG 7.18. Requirements are immediate for 140-3 modules
- End of 2020 – ESVTS available online
- 2021 – Separate scope for established entropy sources

Transition Activities

Workshop on meeting SP800-90B requirements; consistent, uniform expectations of test evidence

Offer pre-review of entropy sources – review of supporting documentation prior to submission for validation

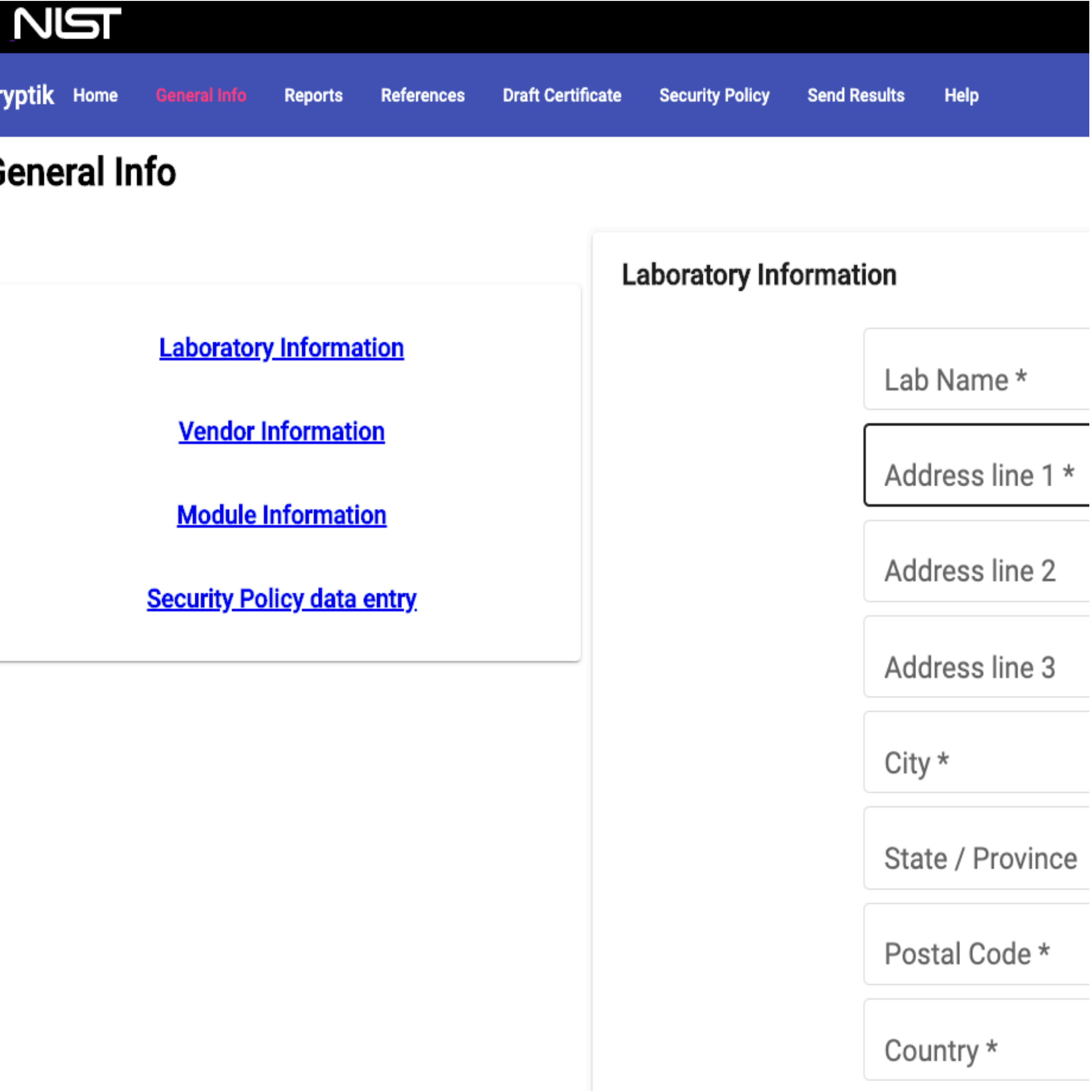
Case Study?

Open review of a public entropy source such as the Linux RNG

What is sufficient evidence to show that noise/entropy source produces the claimed entropy?

What is sufficient evidence in supporting documentation?

ESVTS



eneral Info

Laboratory Information

Vendor Information

Module Information

Security Policy data entry

Laboratory Information

Lab Name *

Address line 1 *

Address line 2

Address line 3

City *

State / Province

Postal Code *

Country *

Similar to ACVTS, ESVTS is a Web API

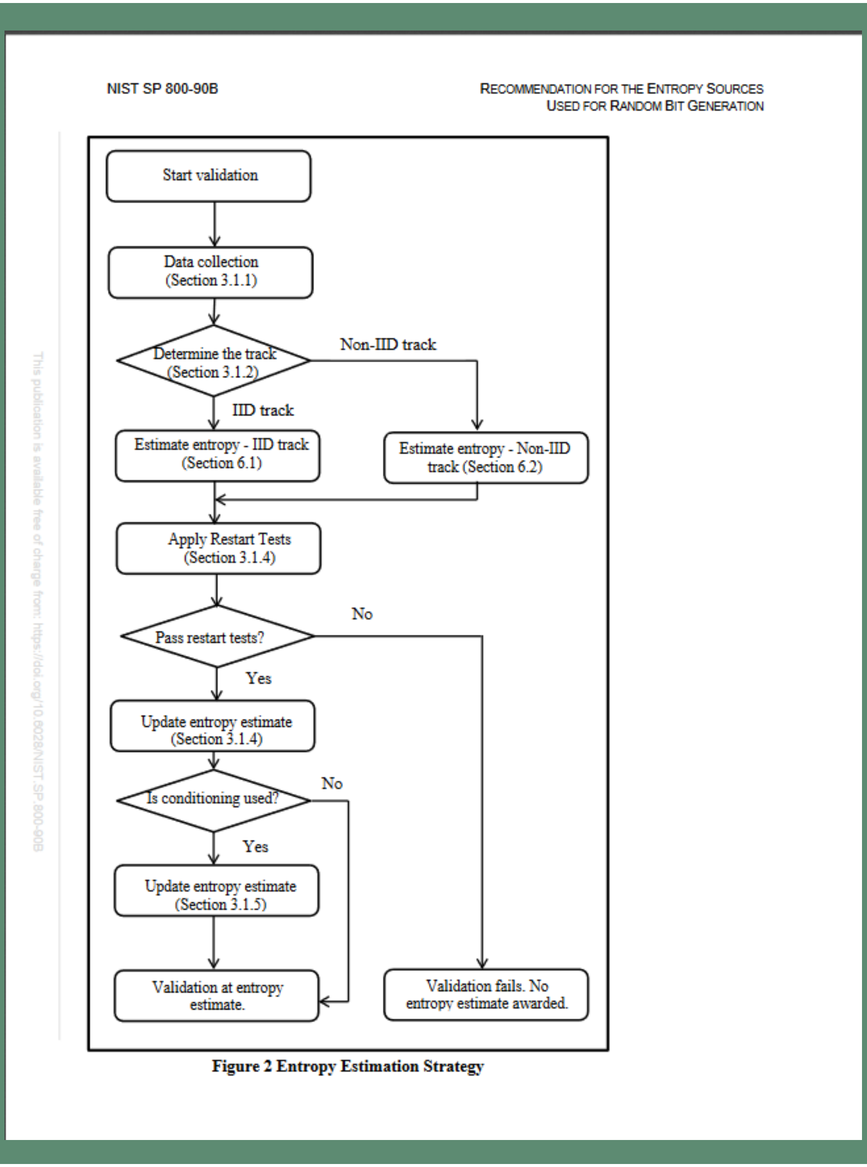
Users upload data files containing raw data, restart data or conditioned data

Server will run the Entropy Assessment Suite against uploaded files

Users upload supplemental data according to IGs 7.18 and 7.19

Client (in development) as a webpage, similar to Cryptik

ESVTS Requirements



NIST SP 800-90B

RECOMMENDATION FOR THE ENTROPY SOURCES
USED FOR RANDOM BIT GENERATION

Start validation

Data collection (Section 3.1.1)

Determine the track (Section 3.1.2)

Non-IID track

IID track

Estimate entropy - IID track (Section 6.1)

Estimate entropy - Non-IID track (Section 6.2)

Apply Restart Tests (Section 3.1.4)

Pass restart tests?

No

Yes

Update entropy estimate (Section 3.1.4)

Is conditioning used?

No

Yes

Update entropy estimate (Section 3.1.5)

Validation at entropy estimate.

Validation fails. No entropy estimate awarded.

Figure 2 Entropy Estimation Strategy

1. Determine IID or non-IID
2. Collect raw noise data
3. Collect restart data
4. List conditioning components
5. Validate vetted conditioning components through ACVP
6. Collect non-vetted conditioning component data
7. Prepare supporting documentation
8. Submit all data to server

Reach Us

Chris Celi – christopher.celi@nist.gov

Tim Hall – CAVP Program Manager – timothy.hall@nist.gov