OpenSSL CONFERENCE

KeyPair CONSULTING

Integrating Multiple Randomness Sources in an SP 800-90C RBGC Framework

Joshua Hill,
KeyPair Consulting

§ PRIVACY AS A FUNDAMENTAL HUMAN RIGHT

20.10.2026

What the What, Now?

20.10.2026

- We examine the implications of the “new” SP 800-90C document.
- We look at an SP 800-90C restriction on the Get_entropy_bitstring() interface and highlight some consequences of this restriction to common design patterns.
- We present a design that resolves many of these issues.
- We discuss some relevant parts of CMVP’s recently proposed draft SP 800-90C IGs.

SP 800-90?

These NIST documents define how randomness can be produced in FIPS 140-3, with likely broader eventual applicability.

20.10.2026

- SP 800-90A defines specific DRBGs (CSPRNGs with specifically designed interfaces and capabilities) which provide computational resistance to attack.
- SP 800-90B defines interfaces and capabilities for Entropy Sources suitable for seeding the SP 800-90A DRBGs.
- SP 800-90C defines a few specific design patterns (RBGs) which combine DRBGs and Entropy Sources.
- In the mid-term (say, 18 months), all key generation in FIPS 140-3 modules will need to occur using validated SP 800-90C RBGs.

Interfaces

SP 800-90C has some requirements placed at the level of abstract interfaces.

- The Get_entropy_bitstring() interface is the only way that 90C constructions get entropy they can credit.
- Get_entropy_bitstring() has some restrictions.

20.10.2026

"The Get_entropy_bitstring process **shall** only be used to access one or more **validated** entropy sources. Any non-validated entropy sources **shall** be accessed by a separate process to avoid possible misuse."

- 90C Section 3.1, Item 1

An Interface Restriction

Abstract interface requirements can impose design restrictions.

20.10.2026

- Many situations exist where a single source base or binary is used across multiple Operating Environments (OEs).
- The validation status of the OEs' Entropy Sources (ESs) varies, and there is little that vendors can do about that.
  - E.g., Intel and AMD RdSeed ESV certificates apply to very specific chips.
  - Many such designs are well-engineered physical noise sources and when such ESs are available their output ought to be integrated into the DRBG internal state as a matter of good engineering practice, even if their output cannot be credited as contributing entropy.

JEnt Limitations

JEnt is a common approach to satisfying the entropy requirements, but it is hardware-dependent and fragile.

20.10.2026

- The Jitter Entropy Library (JEnt) is commonly used in OEs where the underlying hardware ES may or may not be validated.
- Modern JEnt is mostly straightforward to validate for specific hardware, but...
  - It is a classic non-physical (found) Entropy Source and developing a conservative entropy bound for it is fraught.
  - It requires configuration based on hardware-specific testing.
  - The resulting validations are fragile and are hardware- and configuration-specific.

Multiple OE Flexibility

Complying with CMVP requirements should not result in a less secure system.

20.10.2026

- To account for the shifting ES validation status across multiple OEs / implementations, we need a way to combine the contributions of validated and non-validated ESs.
  - The validation status of each ES may not be known by the implementation *a priori*, but…
  - Validation status of these ESs for all evaluated OEs will be known and verified during the 90C (and FIPS) validation.
- Vendors seeking ease of validation commonly exclude reasonable ESs for transient validation status reasons.
  - This effectively incentivizes brittle designs to reduce validation effort.

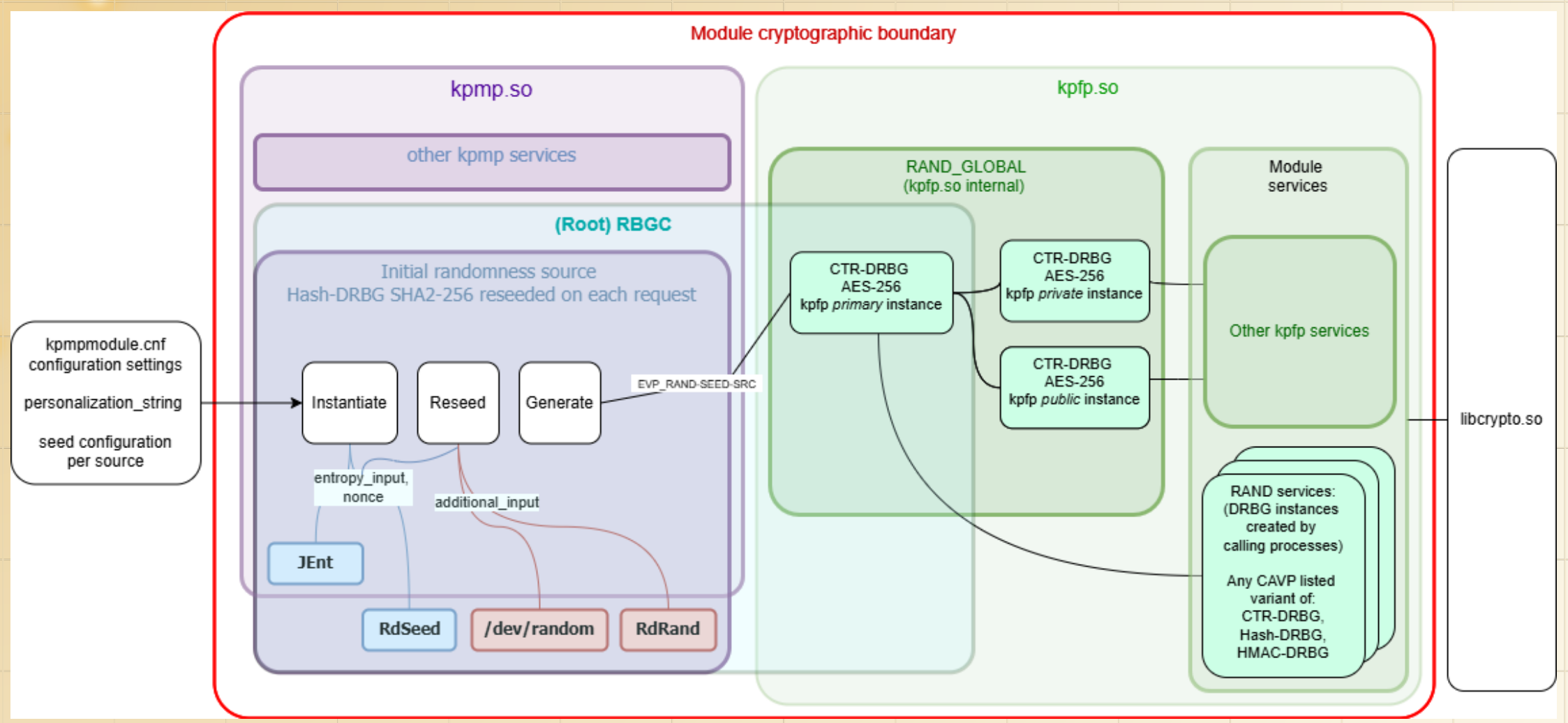
A Modest Proposal

20.10.2026

OpenSSL CONFERENCE

We propose a solution that:

- Offers SP 800-90A/B/C compliance using a full RBGC construction.
- Addresses the Get_entropy_bitstring() non-validated entropy source exclusion issue.
- Is easily integrated into existing libraries.
  - Many libraries (and their users) presume that all seeds are full entropy.
  - Most libraries lack a centralized infrastructure for distributing *additional_input*.
- Is configurable to support multiple OEs.
  - Make the implementation invariant and push OE-specific details to configuration.



Our Proposed Solution

The RBGC Initial Randomness Source

20.10.2026

OpenSSL CONFERENCE

The RBGC Initial Randomness Source (IRS) RBG is central to the RBGC Root construction. To address these goals, it should:

- Produce strings that are either full entropy or have a defined security strength.
- Integrate input from all available healthy ESs, both validated and non-validated.
  - Compliantly segregate the output of validated ESs from the output of other ESs.
  - Use a conservative DRBG design that cryptographically integrates *additional_input*.
- When multiple validated ESs are available, degrade gracefully in the event of failures.

The RBGC IRS

Decisions, Decisions!

20.10.2026

The RBGC Initial Randomness Source (IRS) RBG implemented here:

- Uses a SHA2-256 Hash_DRBG with a security strength (s) of 256.
- Is an RBG that can be configured to:
  - Be (or act “much like”) a fault-tolerant RBG3(RS),
    - Only physical entropy sources can be counted for a true RBG3(RS).
    - In this mode, if the only validated ESs are non-physical, this results in an RBG2(NP) with prediction resistance for every request.
  - Or be a compliant RBG2.
- DRBG Instantiation is similar for the two cases.
  - A personalization string is provided by configuration.
  - $3s/2$ bits are provided from each validated entropy source.

The RBG2 Mode

Conservative and compliant.

20.10.2026

- The RBGC IRS is an RBG2, which establishes its reseed requirements.
  - On reseed, all of the healthy validated ESs have an opportunity to contribute s (256) bits of entropy.
  - There must be a Reseed operation if 2^{17} or more bits were output since the last reseed / instantiate.
  - If adequate entropy from validated ESs is present in a FIFO when a Generate is requested, then a Reseed is opportunistically performed.
  - Otherwise, buffered output from the non-validated ESs can still be integrated into the Generate function as *additional_input* (n.b.: this does not count as a "reseed" for the reseed cadence requirements).
- The DRBG generate size restrictions are enforced on a per-generation basis.

The RBG3(RS)-Like Mode

An extra assurance mode.

20.10.2026

- The RBGC IRS DRBG reseed cadence is the same as for the DRBG in an RBG3(RS).
  - Every generate is preceded by a (RBG3(RS)-Method-A style) Reseed.
  - s+64 (320) bits of entropy are requested from **each** of the healthy validated ESs.
- The RBG3(RS) DRBG generate size restrictions are enforced.
  - The RBGC IRS RBG DRBG produces at most s (256) bits per generate.

Reseed Similarities

In all cases, we use data from all available entropy sources.

20.10.2026

OpenSSL CONFERENCE

In both cases:

- The *seed_material* for the Reseed is the concatenation of the entropy strings produced by the healthy validated ESs.
- The RBGC IRS RBG also uses similar amounts of information from the non-validated ESs as *additional_input* for the Reseed.

Recent Developments

Certain IG drafts are relevant.

20.10.2026

OpenSSL CONFERENCE

The Draft IG D.T ENT.1 allows somewhat more flexibility in Get_entropy_bitstring():

- This only applies to RBGC constructions; it is unclear if this will apply to the IRS, which must itself be validated as an RBG2 or RBG3(RS).
- This only includes an allowance for ESs that are validated on some covered platform.
- This imposes additional error handling requirements.

The Cryptographic Boundary and the RBGC

Draft IG D.U allows only certain relationships between the cryptographic boundary and RBG boundary.

20.10.2026

OpenSSL CONFERENCE

- Each RBG has a boundary, and the relationship between this RBG boundary and a cryptographic boundary is discussed in the draft IG D.U.
- The RBGC Root definitionally contains the IRS (and its entropy sources) and the RBGC root DRBG.
- The RBGC and FIPS module must be contained within the same “computing platform” (TOEPP for software/firmware modules).
- The cryptographic boundary must contain:
  - The entire RBGC Root (including the IRS), or
  - An RBGC root DRBG which is seeded using data that crosses into the FIPS module, or
  - An RBGC non-root DRBG which is seeded using data that crosses into the FIPS module.
- When such data crosses the cryptographic boundary, the appropriate SSP I/O requirements apply.

That the That, Now!

SP 800-90C compliance can result in security improvements.

20.10.2026

- Use every entropy source but credit only the validated ones.
- Use the same binary and source base across many platforms and configure them on a per-platform basis.
- One IRS, two modes.
- CMVP is moving toward requiring SP 800-90C RBGs.

Thanks!

Any Questions?