Clarification to the Entropy Documentation and Assessment Annex

Release 2, April 2024

This information is provided for clarification and informational purposes and should not be considered comprehensive guidance, nor used as a checklist for entropy requirements in NIAP-approved Protection Profiles.

The generation of random bits continues to be vital for key generation and the security strength of our cryptosystems. During analysis of different products, discoveries of weak random values make the remaining security measures irrelevant. There has been significant research into generating pseudorandom bits using a Deterministic Random Bit Generator (DRBG) and an unknown seed value. To provide guidance on best practices and testing of entropy implementations and ensure that bits with suitable entropy are input into various DRBG implementations, NIST published the NIST SP 800-90 series to describe entropy sources, RBGs, and their security properties. These also provide tests that can be used to validate the quality of an entropy source. Similarly, Protection Profiles and Common Criteria evaluations moved towards validation of the entropy underpinning the cryptographic strength of validated products. The first step, within NIAP, was the Entropy Assessment Report (EAR).

More recently, NIST established a formal Entropy Validation Program (ESV). Since then a number of entropy sources have successfully obtained ESV certificates. Given this, the method and requirements used by NIAP in evaluating entropy sources (and EARs) is also updated.

NIAP EAR Review Overview

For every EAR submitted, NIAP examines the documentation to verify that the entropy is described completely, from the raw noise source to the seeding of the DRBG or use in cryptographic operations. It is crucial that the EAR documentation shows a sufficient understanding of the source being used and any conditioning performed. If there is an incorrect or unclear description of the source, the entropy justification, or how/where the entropy is used, updated documentation is required before the product is accepted into evaluation.

Going forward, it is expected, per NIAP Policy 5, that ESV certificates are included as part of EAR review. The ESV certificate provides the evidence for the entropy justification, but does not remove the requirement for the rest of the EAR – description of the source and any conditioning is still needed. How entropy gets from the source to the DRBG, without reduction in the entropy estimate provided in the ESV, must also be included. Entropy claims without ESV support and EAR justification will not be accepted. This is especially true for any full entropy claims.

This shifts the focus of the EAR as, traditionally, the most detailed sections of the EAR provided a justification of the entropy provided by the given source. Since the ESV certificate provides the (min) entropy estimate, it is expected that this will reduce the need to provide detailed min-entropy justification or test result output. Therefore, the EAR focus should be on ensuring it contains:

1. a description of the raw noise source itself;
2. the ESV certificate providing the (min) entropy estimate;
3. an explanation of any post-processing or conditioning of that entropy; and
4. how and in what conditions the TOE's cryptographic operations use the entropy.

All of this was previously required and is still needed, even with the inclusion of ESV certificates. It is up to the vendor and CCTL to determine if the documentation used for the ESV program is sufficient for submission to NIAP or if a separate document is submitted as the EAR.

Below, for information, are some examples of how the US Scheme reviews EARs for various entropy source types. This is updated to account for the new ESV certificate(s).

Software Source

It is fairly common that EARs contain software sources. ESV certificate(s) must accompany each of the sources included in the EAR. If there are sources for which there are no ESV certificates, no entropy can be credited to those sources and the description will need to contain a description of the interaction of these sources on the sources with ESV certificates and justification that entropy is not degraded or impacted in any way. EARs with software entropy sources that contain a raw noise source component (e.g. timestamps) must include a min-entropy estimate for the raw noise source; min-entropy test results on the output of the conditioned entropy will not be acceptable.

Self-Provided Hardware Source

Review of EAR documentation indicating that the product provides its own hardware source is treated much the same as for software sources – a sufficient understanding of the source being used and any conditioning performed must be shown for a product to be accepted into evaluation. The ESV certificate associated with the source must be referenced and the description of how the entropy provided is carried through to the DRBG input must be clear.

Third-Party Source

Previously, NIAP guidance allowed for an "assumption" of the entropy provided by a third-party source due to limited access to design and raw entropy data. However, the intent was always to require that third-party sources be evaluated. With NIST's launch of ESV, independent testing, review and certification of entropy sources is now available. This is especially important for third-party sources – the source and applicable ESV certificate must be referenced for any third-party claim; assumption of entropy without ESV certificate support will not be accepted. Pay particular attention to the re-use status on the ESV certificate prior to using one as evidence for a third-party source. With the appropriate ESV certificate referenced, the EAR then describes the use of this source/entropy within the product and justifies that entropy is in no way impacted through the integration of the third-party source within the particular implementation.

Common Problematic Areas

Regardless of the type of entropy source claimed, there are common areas where EARs often fall short, requiring the documentation to be resubmitted for NIAP review prior to acceptance into evaluation. These are outlined below in order to offer some additional guidance. For guidance on Saved State, please see the previous Clarification document.

Seeding

It is expected that vendors will pursue and obtain ESV certificates, requiring them to collect a large number of raw source bits, perform statistical tests, and from those statistical tests obtain a rate of entropy. ESV requires particular statistical tests, as described in NIST SP 800-90B, to determine the amount of entropy in each output. The EAR documentation must then provide enough detail to verify that the DRBG is initialized with the entropy stated in the ST, given the entropy estimate per output and the amount of source data used to seed the DRBG. If the amount of source data used to seed the DRBG is not clear or the calculated rate is not explicitly related to the seed, the vendor is required to resubmit the EAR documentation.

Linux Kernel DRBGs

In 2020, updates to the LKRNG in the Linux Kernel removed the blocking pool. This, along with previous updates that added an algorithm that is not NIST approved, resulted in several EAR rejections. There is a path by which these implementations can still be approved, given appropriate mitigations to address the changes in the LKRNG, but be aware that this often requires several rounds with the EAR Review Team.

Application Use of Platform Random

Several NIAP PPs include a “platform-based DRBG” source option as part of the FCS_RBG requirements. This supports the use of a third-party source, particular for application use of platform random. It should be noted, however, that this selection can only be made when the platform random is used directly by the application. It cannot be used, for example, when the random values provided by the platform are used to seed other DRBGs or when the values are further processed or conditioned by the application prior to use. When using to seed other DRBGs, an EAR as well as certificates for the DRBG are required, and when further processed an EAR is needed to ensure entropy is appropriately maintained. This likely means that “invoke platform provided DRBG” is not the appropriate selection. Any questions or requests for additional information by the validation team to ensure the “platform-provided” selection is used properly must be addressed for successful validation. While there is currently no EAR requirement when “platform-based DRBG” is selected, it is acceptable to provide such processing or design information in an EAR anyway, should the vendor not want this description available in the public ST.