CKG Guidance related to SP800-Br1 and associated tables

IG D.H - Requirements for Vendor Affirmation to SP 800-133

- Vendor affirmation to SP 800-133 is required for all methods covered by Sections 4 and 6.3 of this standard; that is, when a symmetric key or a seed for asymmetric key generation is generated starting with a random bit string. The module's validation certificate **shall** have a CKG entry only if the module is generating keys for the symmetric-key algorithms. Only one CKG entry is required for the module's certificate, even if the module employs multiple key generation methods that must be documented in the certificate. The Security Policy **shall** provide the details of each method.

This IG guidance can't apply directly to Br1 submissions as there is no longer a separate validation certificate entry. The certificate information is generated directly from the tables associated with the Security Policy.

CKG entries for both symmetric and asymmetric vendor affirmed cases should be included in Table 6 – Vendor Affirmed Algorithms.

There should be separate entries for symmetric and asymmetric vendor affirmed claims.

There should be multiple symmetric or asymmetric entries only if there are multiple distinct approaches used by the module. For example, if there are different types of asymmetric key-pairs generated that use the same reference example from SP800-133r2 Section 4 or method from Section 6, there should only be one asymmetric CKG entry.

The entries in Table 6 – Vendor Affirmed Algorithms should follow these conventions:

- Algorithm Name – Unique for every entry and include "CKG"
- Algorithm Properties
    - Name: "Key Type"
    - Value: "Symmetric" or "Asymmetric"
- Implementation – N/A
- Reference – List the corresponding example/section and item within SP800-133r2
    - Section 4, examples 1 through 4 or other with explanation
    - Section 6.3, approved methods 1, 2, or 3
    - If there is post-processing of the U value prior to applying the CKG approach, include the details

If there is a service that provide symmetric key generation, create an entry in the SFI table with the "CKG" type and include the Table 6 entry in the Algorithms column. For an asymmetric key generation entry in the SFI table, use the AsymKeyPair-KeyGen type.