Legacy Random Number Generators (RNGs)

Zhiqiang “Richard” Wang

Leidos CSTL

NVLAP Lab Code: 200427-0

Reminder

- **Legacy RNGs transition period will be ended on December 31, 2015.**

Overview

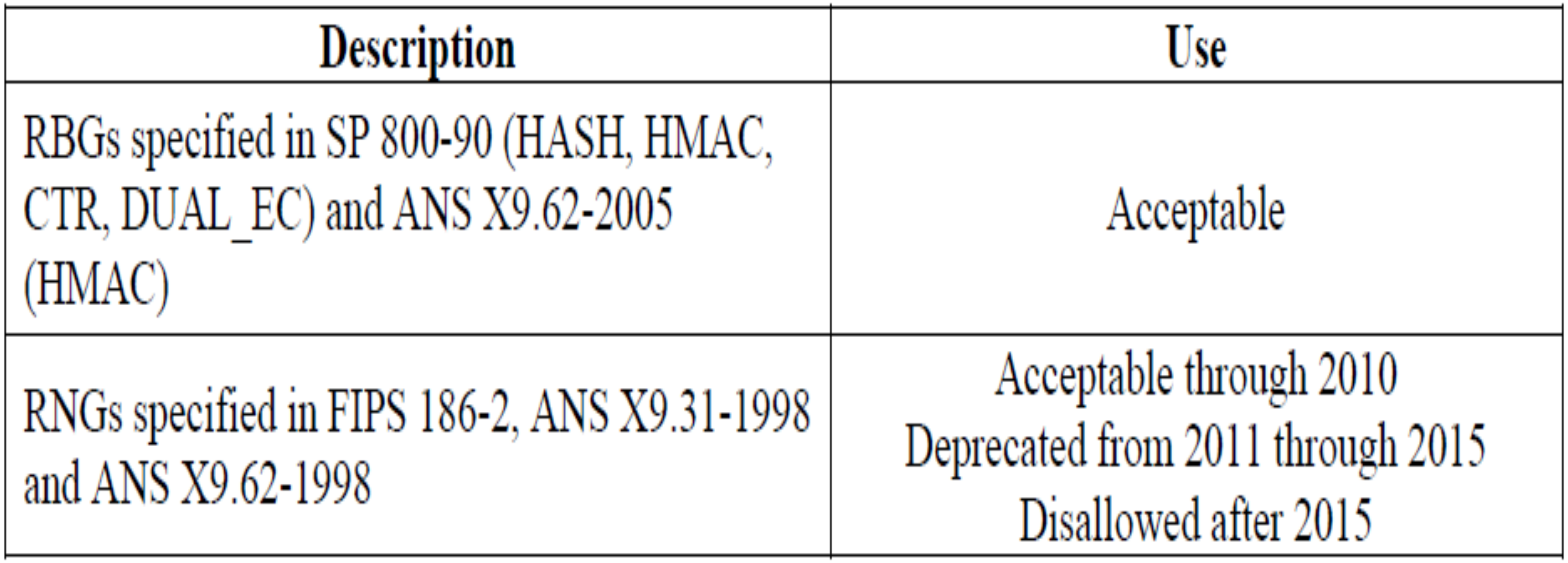
- High level introduction to Legacy Random Generators (RNGs) and DRBG – by Richard Wang (Leidos)
- Security strength comparison between the legacy RNGs and DRBG – by Richard Wang (Leidos)
- How a CSTL Lab (Leidos) will handle the RNG change – by Richard Wang (Leidos)
- Information that Leidos learned from CAVP and CMVP about the RNG change – by Richard Wang (Leidos)
- A Vendor Perspective about the RNG change – by William Tung (Gemalto)

High level introduction to Legacy Random Generators (RNGs) and DRBG

- What do the Legacy RNGs include?
  - FIPS 186-2 RNG
    - General Purpose RNG
    - Regular 186 RNG
  - ANSI 9.62 RNG -1998
    - P Curves (P-192/224/256/384/521)
    - K Curves (K-163/233/283/409/571)
    - B-Curves (B-163/233/283/409/571)
  - FIPS X9.31 RNG -1998
    - Using 2-Key/3-Key Triple-DES Algorithm
    - AES (128/192/256) Algorithm

High level introduction to Legacy Random Generators (RNGs) and DRBG (cont.)

- What approved RNGs shall be used in FIPS mode after 2015?
  - Table 3 from SP800-131 (released on January 2011):

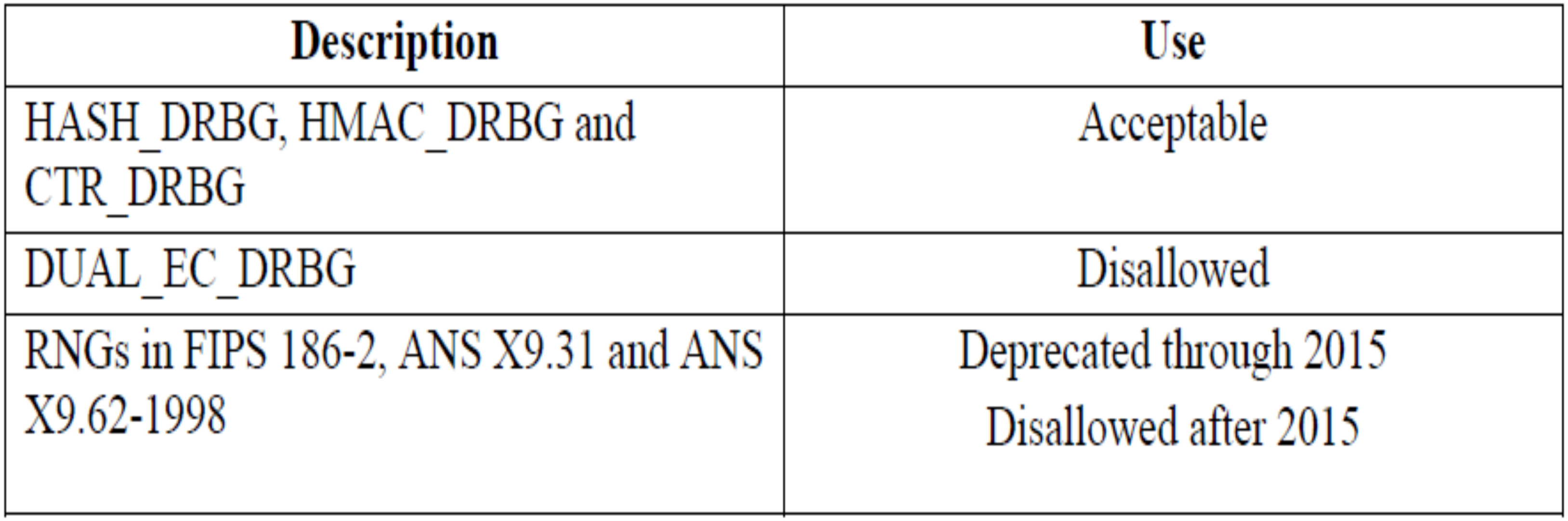


Description	Use
RBGs specified in SP 800-90 (HASH, HMAC, CTR, DUAL_EC) and ANS X9.62-2005 (HMAC)	Acceptable
RNGs specified in FIPS 186-2, ANS X9.31-1998 and ANS X9.62-1998	Acceptable through 2010 Deprecated from 2011 through 2015 Disallowed after 2015

Note that in 2005, a revision of [X9.62] was approved that includes the HMAC_DRBG specified in [SP 800-90], and does not include the RNGs in the 1998 version.

High level introduction to Legacy Random Generators (RNGs) and DRBG (cont.)

- Table 3 from (Draft) SP800-131a (released on July 2015):



Description	Use
HASH_DRBG, HMAC_DRBG and CTR_DRBG	Acceptable
DUAL_EC_DRBG	Disallowed
RNGs in FIPS 186-2, ANS X9.31 and ANS X9.62-1998	Deprecated through 2015 Disallowed after 2015

- HMAC_DRBG in ANSI X9.62-2005 was removed
- DUAL_EC DRBG was removed

High level introduction to Legacy Random Generators (RNGs) and DRBG (cont.)

- SP800-90a DRBG shall be used in FIPS mode after 2015
  - DRBGs in SP800-90a Revision 1
    - HASH_DRBG (SHA-1, SHA-224, SHA-256, SHA-384, SHA512, SHA-512/224 and SHA-512/256)
    - HMAC_DRBG (HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA512, HMAC-SHA-512/224 and HMAC-SHA-512/256)
    - CTR_DRBG (3Key Triple-DES, AES-128. AES-192 and AES-256)

Security Strength Comparison Between the Legacy RNGs and DRBG

- Desired Security Strength Supported by Legacy RNGs
  - No desired security strength is supported.
  - There is no entropy requirement in the seed, only the seed length needs to meet the requirement. For example:
    - FIPS 186-2 RNG using SHA-1 as G Function requires 20~64 bytes seed value
    - FIPS 186-2 RNG using DES as G Function requires 20 bytes seed value
    - ANSI 9.62 RNG -1998 requires 20~64 bytes seed value
    - ANSI X9.31 Appendix A.2.4 Using 3-Key Triple DES requires the 8 bytes seed value
    - ANSI X9.31 Appendix A.2.4 Using AES requires the 16 bytes seed value

Security Strength Comparison Between the Legacy RNGs and DRBG (cont.)

- Desired Security Strength Supported by DRBG. (Pleaser refer to SP800-90a and SP800-57)
  - HASH_DRBG and HMAC_DRBG
    - SHA-1 → 112/128 bits
    - SHA-224 and SHA-512/224 →112/128/192 bits
    - SHA-256 and SHA-512/256 → 112/128/192/256 bits
    - SHA-384 → 112/128/192/256 bits
    - SHA-512 → 112/128/192/256 bits
  - CTR_DRBG
    - Triple-DES → 112 bits
    - AES 128 bits →128 bits
    - AES 192 bits →192 bits
    - AES 256 bits →256 bits

How Leidos will Handle the RNG Change

- To ask vendor to provide the detailed information about the changes made by the vendor.

- To analyze and decide which scenario (IG G.8, 1SUB/2SUB/3SUB/4SUB/5SUB) the re-validation can fall into for CMVP submission.

- To perform the documentation reviews to make sure the accuracy of DRBG implementation

- To have DRBG CAVS tested and get the results submitted to CAVP for certification

How will Leidos Handle the Change (Cont.)

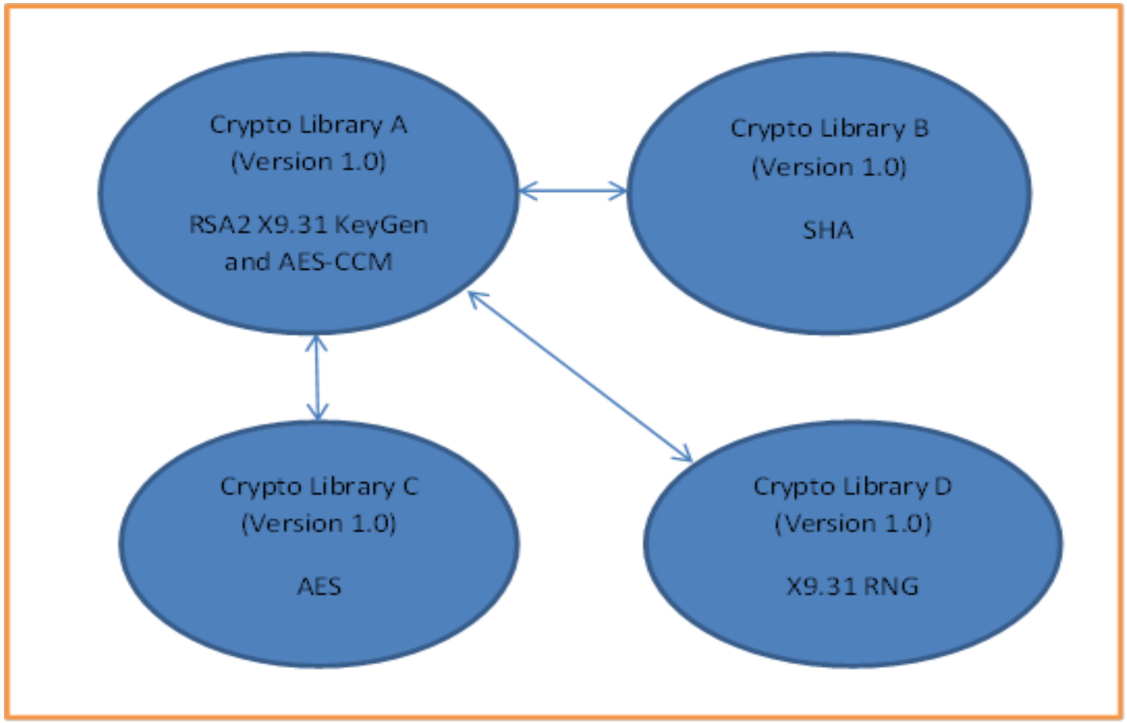
- To review and assess the vendor provided entropy report if needed.
- To perform regression operation tests to all security services due to the RNG changes.
- To have the Cryptik Report, Security Policy, Entropy Assessment report, Physical Test Report (if needed) and all other required files submitted to CMVP for certification

Information that Leidos Learned about the RNG Replacement

- CAVP
  - Legacy RNGs will be placed into the "*Historical RNG Validation List*" on CAVP Algorithm Validation Lists.
  - Algorithms using the Legacy RNGs as the prerequisite algorithm will not be allowed in FIPS mode.
  - Algorithm re-tests due to RNG change:
    - Case I: If the module is one monolithic library and it changes due to the DRBG change, then the vendor would have to retest all algorithms in that crypto library.

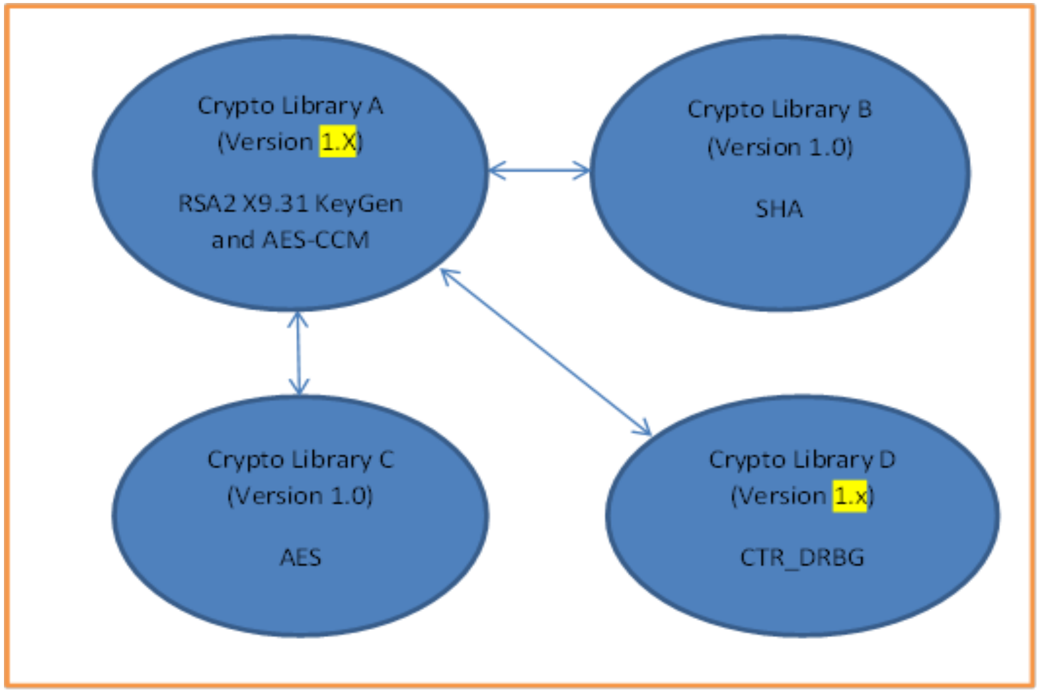
Information that Leidos Learned about the RNG Replacement (Cont.)

- Case II: If the module is a library that is a set of several libraries, then it may be possible to retain some of the older validations.
  - Before RNG change, Library A has the links with Libraries B, C and D



Information that Leidos Learned about the RNG Replacement (Cont.)

- After RNG replacement,
  - Libraries A and D shall have to go through a new round of CAVS tests
  - Library B and D can remain the original versions



Information that Leidos Learned about the RNG Replacement (Cont.)

- CMVP
  - **Validated modules on the CMVP validation lists:**
    - The CMVP will move the X9.31 RNG listings from the approved to the non-approved line on all affected FIPS 140-2 module certificates.
    - If after removing the RNG's from the approved line there is at least one remaining approved algorithm, the module certificate will **not** be revoked. A module transition note may also be provided, similar to the notes for the end-of-2013 algorithm transitions.

Information that Leidos Learned about the RNG Replacement (Cont.)

- CMVP
  - **Modules on the CMVP queue**
    - REVIEW PENDING or IN REVIEW: The laboratories/vendors will be asked to provide an updated submission that is fully compliant with the transition. Only compliant submission will be validated.
    - COORDINATION: These module submissions will be handled like those in the REVIEW PENDING or IN REVIEW case.
    - FINALIZATION: These module submissions will be handled like already validated modules.
  - **1/2/4 SUBs for validated modules on the CMVP validation lists**:
    - When an updated Security Policy is submitted it will be required to comply with the transition.

gemalto security to be free

SafeNet THE DATA PROTECTION COMPANY

The RNG Transition: A Vendor Perspective

William Tung
November 2015

Things to Consider

- Keys and Keypairs that were generated using the 2016 non-Approved RNGs
  - Considerations for keys that are not meant to be updated (Root CA keys)
  - Handling these persistent keys which must remain because they were generated prior to 2016
  - IVs and Nonces generated using 2016 non-Approved RNGs
  - Key Loading vs. Key Generation
- What if my module only supports a non-Approved RNG in 2016?
- Best course of action:
  - 3SUB?
  - 5SUB?
  - Wait for ISO 19790?

Things to Consider

- Change often leads to opportunity
  - Opportunity for vendors to introduce a new product
  - Opportunity to provide security patches with new RNG
  - Opportunity for labs to perform more validation testing
  - Opportunity for CMVP to re-validate modules

Other Algorithms

- Elliptic Curve Cryptography (ECC) is gaining traction in the market
  - NIST recommends using ECC for stronger key lengths
  - Emerging international preference (Europe) for ECC over RSA
  - NIST approved ECC curves vs. other ECC implementations
  - Increased product support for ECC as a result

Questions

Thank you