SP 800-90A: DRBG Mechanisms
Background/History

- Originally published as SP 800-90 in 2006 and revised in 2007
- Revised as SP 800-90A in 2012 and 2015
- Revised as SP 800-90A Rev. 1 in 2015
  (included removing approval of the Dual_EC_DRBG)
• Security strengths: support 112, 128, 192, or 256 bits

• Boundaries

• Internal state:

<table>
<thead>
<tr>
<th>Internal State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working state</td>
</tr>
</tbody>
</table>

• Backtracking and prediction resistance
• Instantiate: Initial seed $\rightarrow$ internal state

• Reseed: (New) seed $\rightarrow$ internal state

• Generate: Request bits $\rightarrow$ produce output

• Uninstantiate: Destroy internal state when DRBG is no longer to be used
Instantiate Function

- **entropy input**
- **nonce**

requested_instantiation_security_strength

(Opt.) prediction_resistance_flag

(Opt.) personalization_string

Instantiate function

- status
- state_handle

Internal state
Seed Construction for Instantiation

entropy input || nonce || (opt.) personalization string

Note: In most cases, the entropy input need not have full entropy
Reseed Function

- **entropy input**
- **state_handle**
- *(Opt.)* **additional_input**

Reseed function

- **status**

Internal state
Seed Construction for Reseeding

internal state value(s) || entropy input || (opt.) additional input
Generate Function

Reseed_function

? → state_handle

requested_number_of_bits → requested_security_strength

(Opt.) prediction_resistance_request → (Opt.) additional_input

Generate function

status → pseudorandom_bits

Internal state
Uninstantiate Function

Uninstantiate function

state_handle \rightarrow Uninstantiate function \rightarrow status

Destroy internal state
Functional Model

- Personalization String
- Additional Input
- Nonce
- Entropy Input
- Instantiate
- Reseed
- Internal State
- Uninstantiate
- Tests
- Error State
- Generate
- Pseudorandom Output

Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
DRBG Algorithms

- Hash-based: Hash_DRBG and HMAC_DRBG:
  - Use SHA-1 or SHA-2

- Block-cipher-based: CTR_DRBG:
  - Use 3TDEA or AES
    - Variants: with or without a derivation function (df); no df requires full entropy

- Tables provided for function parameters
Other Stuff

• Implementation assurances via lab testing:
  o Documentation requirements
  o Conformance testing
  o Health testing

• Appendices:
  o Conversion routines, examples, DRBG mechanism selection, revision history
Proposed Changes for Rev. 2

• New template
• Terminology changes
• Use “Must“ and “must not” for non-testable requirements
• TDEA, SHA-1, and 112-bit security strength removed
• Add SHA-3 (parameters under discussion)
Proposed Changes (cont’d.)

• Recommendation added to employ an “atomic” generate operation

• Instantiate, reseed, and generate functions have been simplified

• The \texttt{Get\_entropy\_input} function (renamed as a \texttt{Get\_randomness-source\_input} function) is a placeholder
• “Nonce” no longer used during instantiation
• Replaced by additional bits from the randomness source
  o Entropy source: 3/2 (security strength) bits of entropy
  o RBG: bit string 3/2 (security strength()) bits long

Proposed Changes (cont’d.)

Randomness Input

Nonce

(Optional) Personalization String

Seed

randomness input || (opt.) personalization string
Proposed Changes (contd.)

- Hash\_DRBG and HMAC\_DRBG
  - Table modified: remove SHA-1; add SHA-3

- CTR\_DRBG
  - Table modified: remove 3TDEA
  - Two new derivation functions added

- Figures added

- Examples will be updated
Questions?
Thanks!