SP 800-90A: DRBG Mechanisms

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

INFORMATION TECHNOLOGY LABORATORY

Background/History

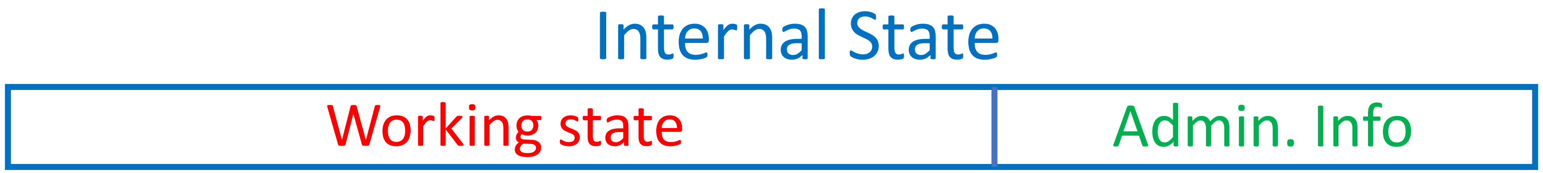
- Originally published as SP 800-90 in 2006 and revised in 2007
- Revised as SP 800-90A in 2012 and 2015

- Revised as SP 800-90A Rev. 1 in 2015

  (included removing approval of the Dual_EC_DRBG)

SP 800-90A Contents

- Security strengths: support 112, 128, 192, or 256 bits
- Boundaries
- Internal state:



Internal State

Working state

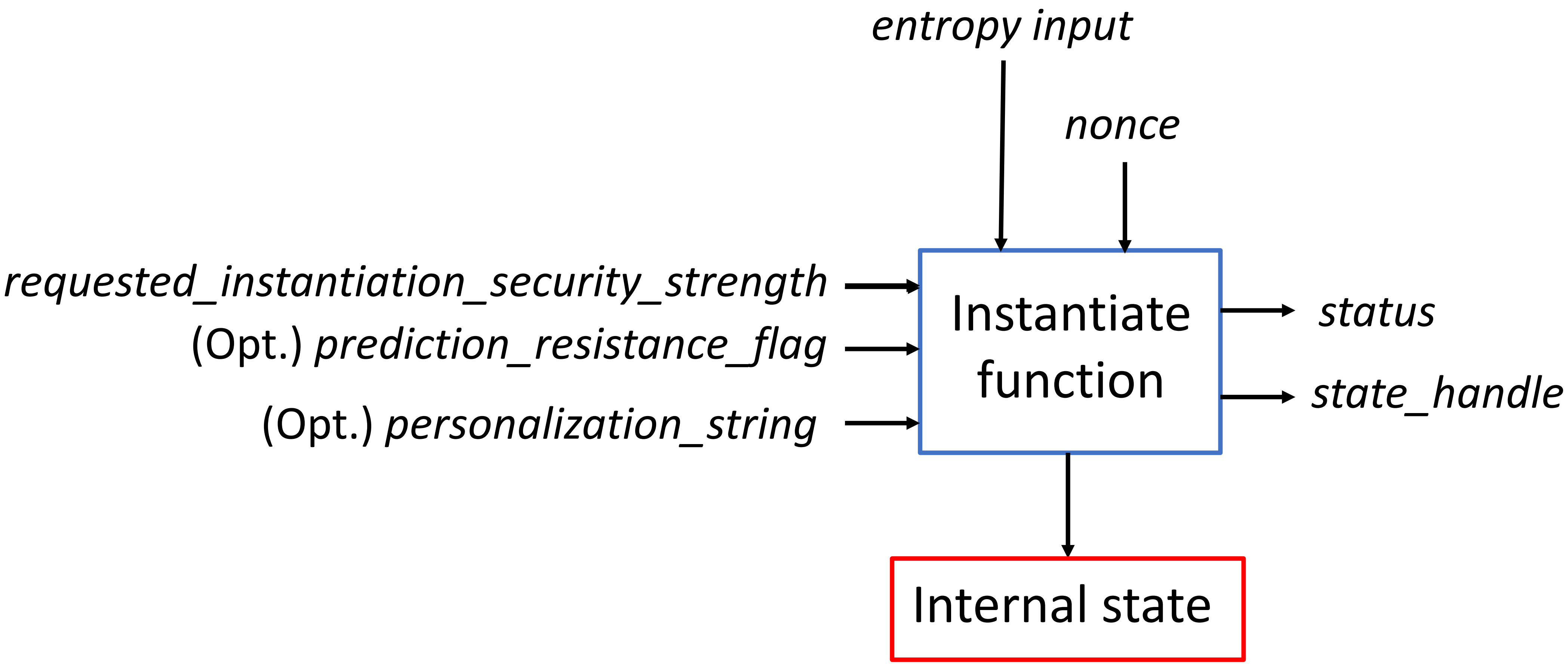
Admin. Info

- Backtracking and prediction resistance

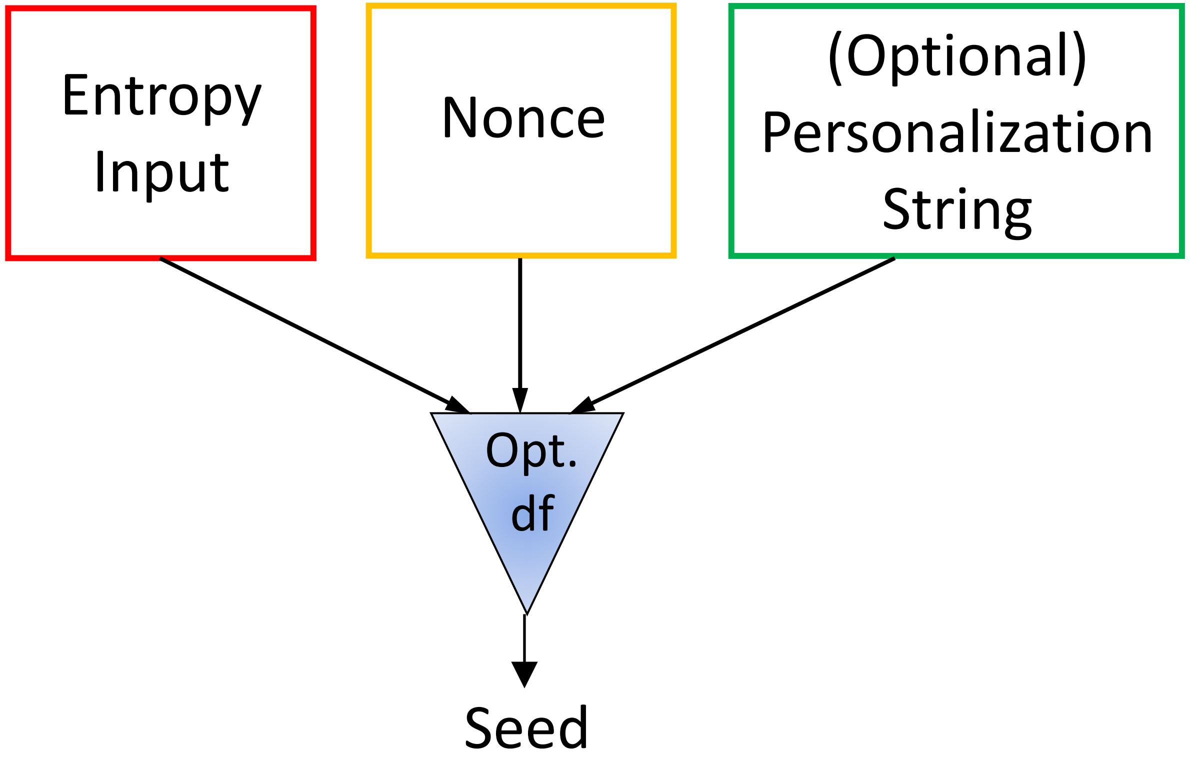
(General) Functions

- Instantiate: Initial seed → internal state
- Reseed: (New) seed → internal state
- Generate: Request bits → 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

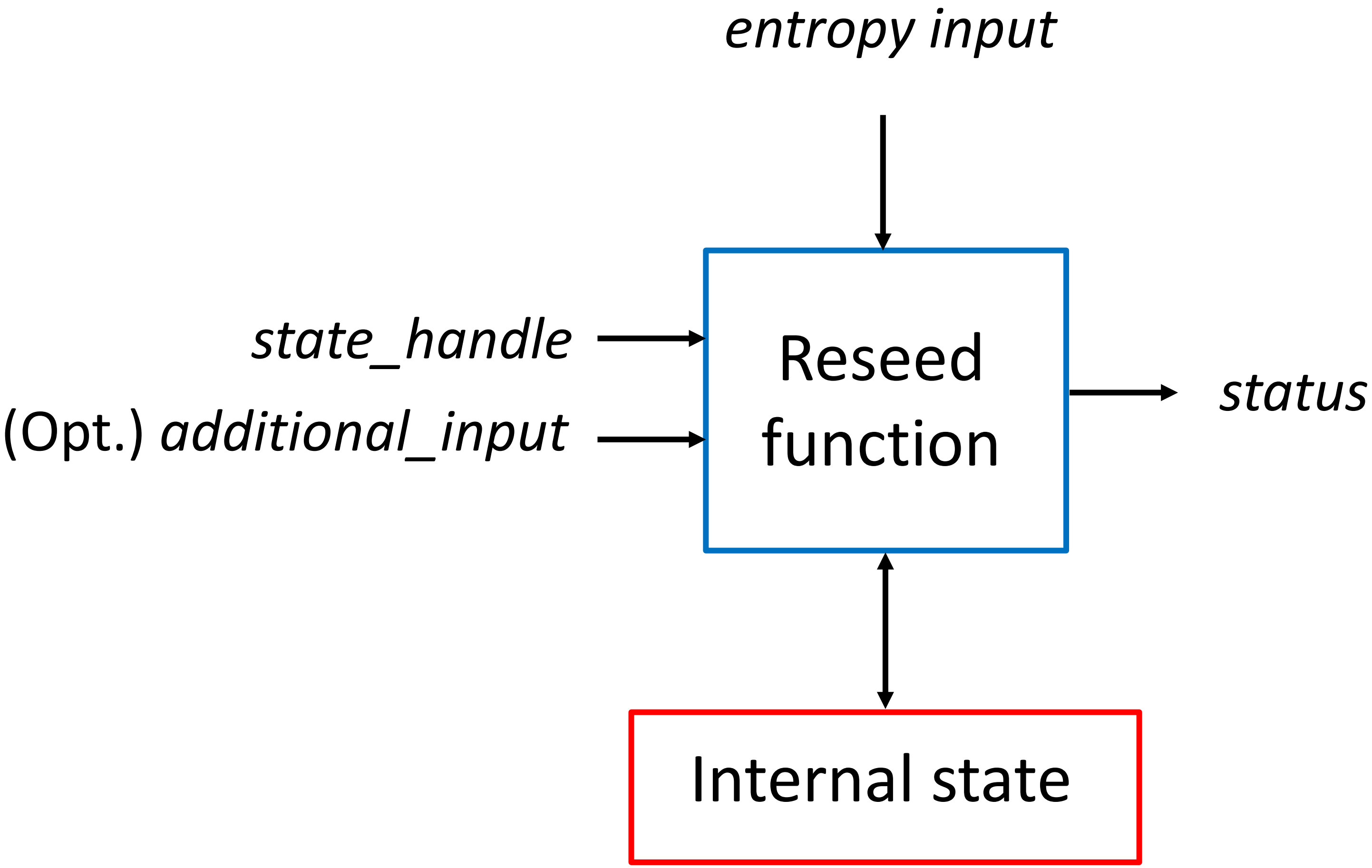
Seed Construction for Instantiation



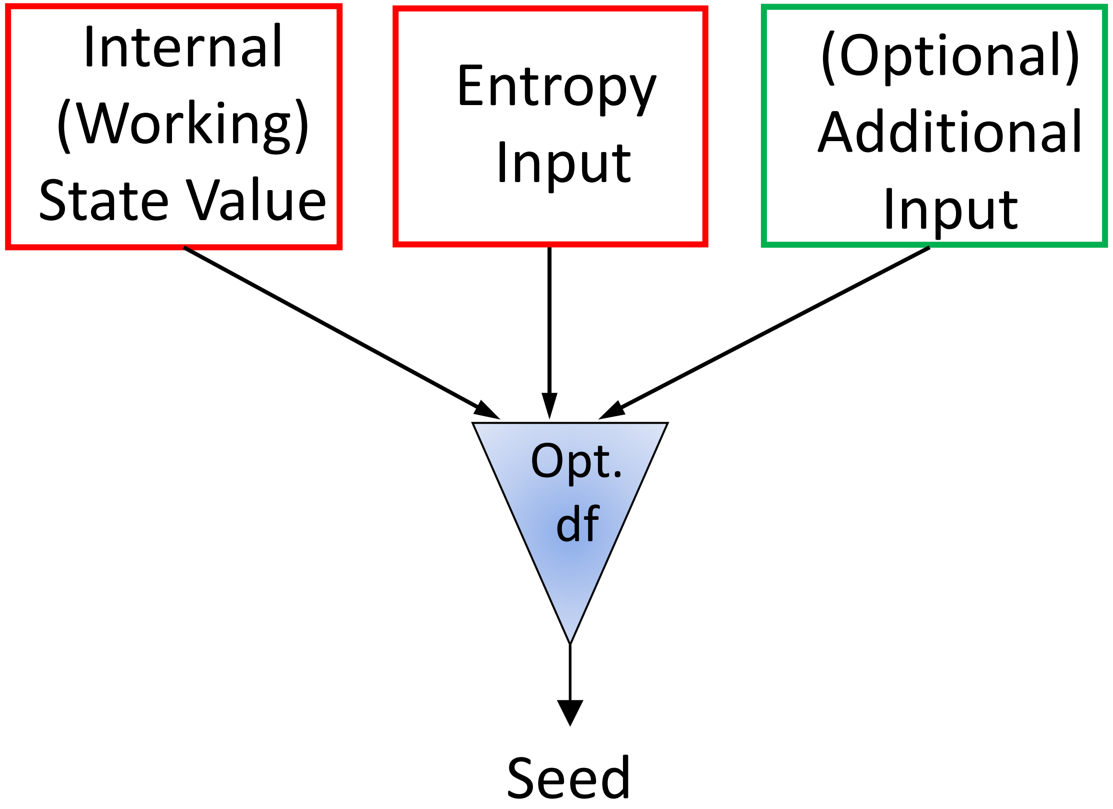
Note: In most cases, the entropy input need not have full entropy

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

Reseed Function

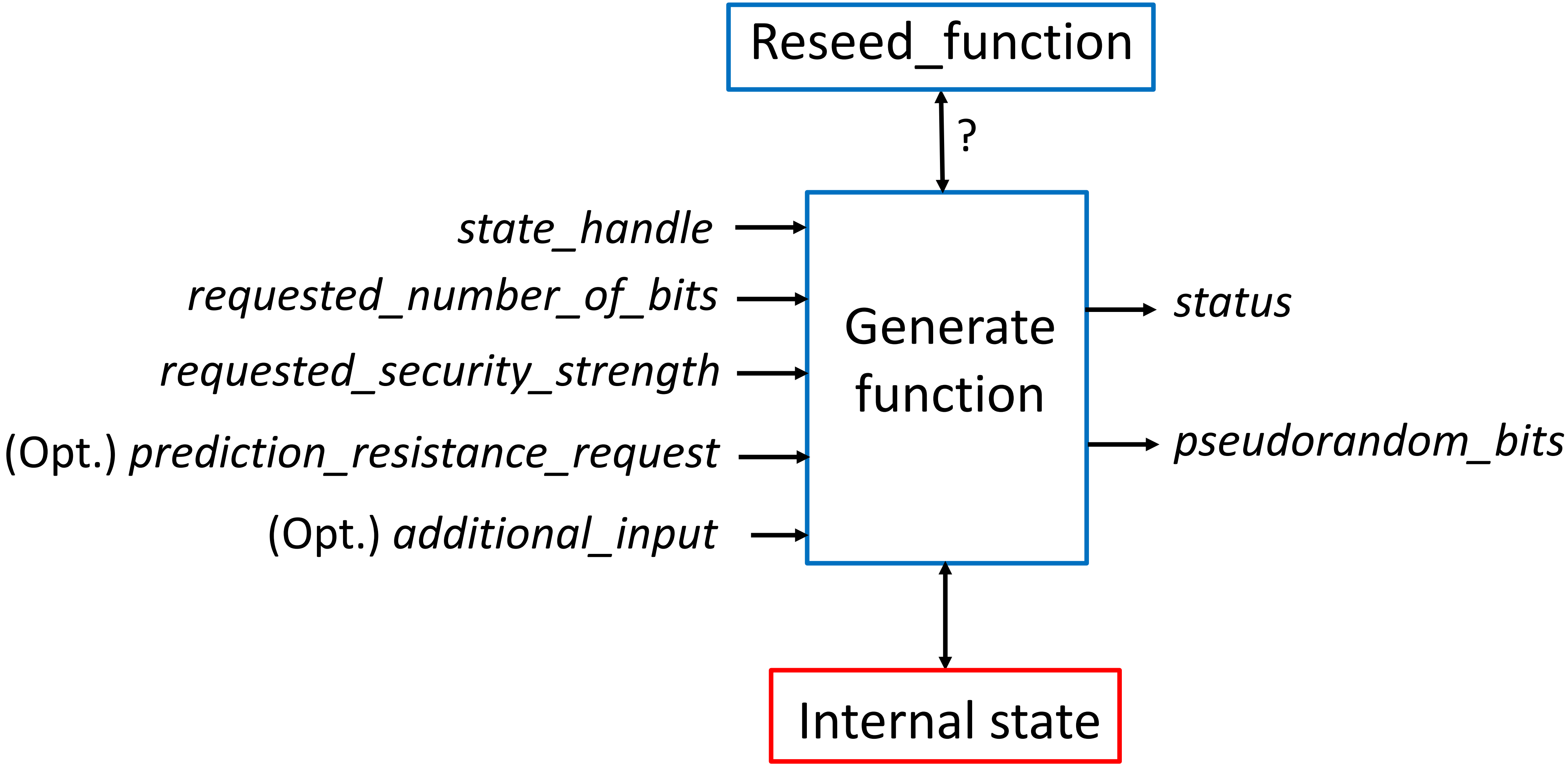


Seed Construction for Reseeding

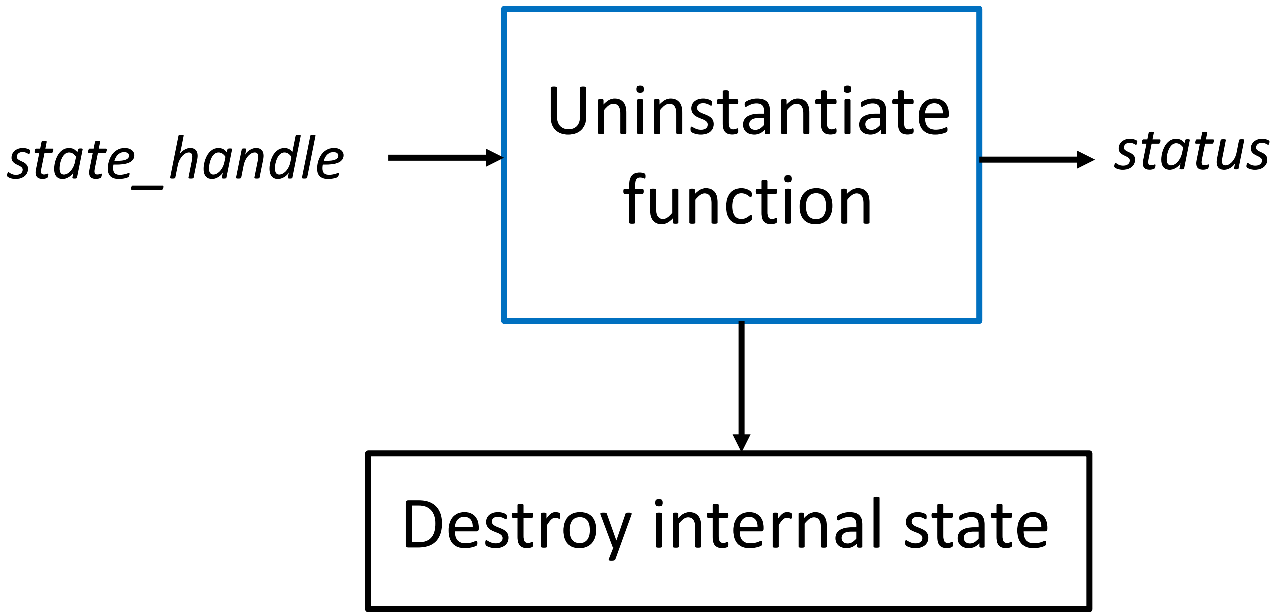


internal state value(s) || entropy input || (opt.) additional input

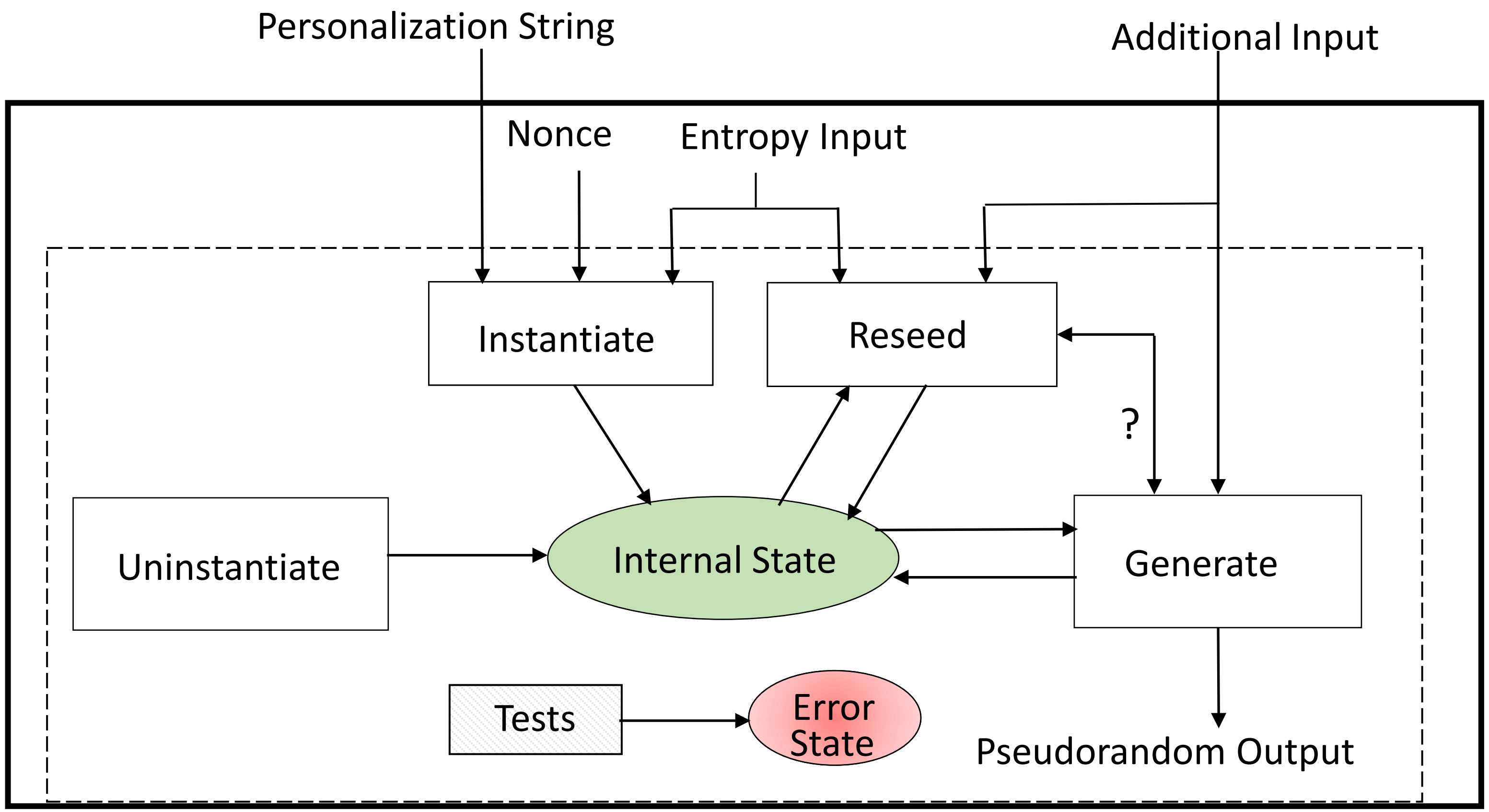
Generate Function


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



Functional Model



❖ 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:
  - Documentation requirements
  - Conformance testing
  - Health testing
- Appendices:
  - Conversion routines, examples, DRBG mechanism selection, revision history

Proposed Changes for Rev. 2

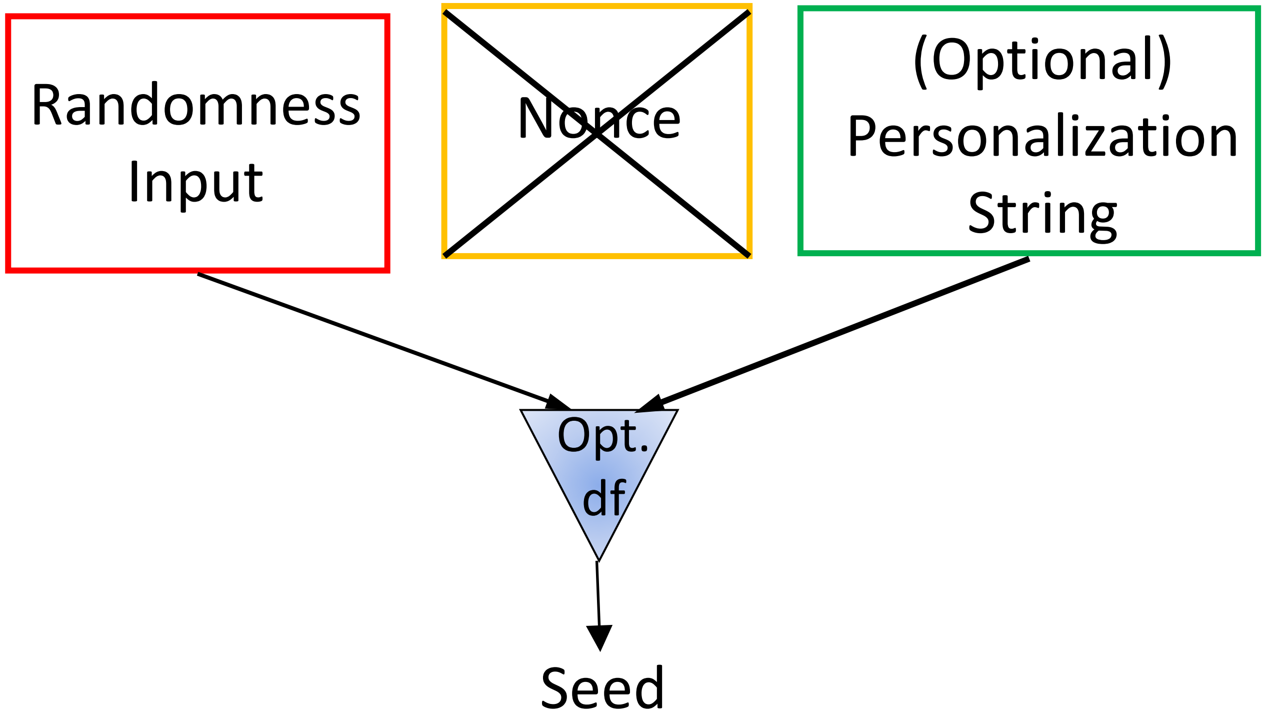
- New template
- Terminology changes
- Use “Must“ and “must not” for non-testable requirements
- TDEA, SHA-1, and 112-bit security strength removed
- Add SHA-3 (parameters under discussion)

Proposed Changes (cont'd.)

- Recommendation added to employ an "atomic" generate operation
- Instantiate, reseed, and generate functions have been simplified
- The **Get_entropy_input** function (renamed as a **Get_randomness-source_input** function) is a placeholder

Proposed Changes (cont'd.)

- "Nonce" no longer used during instantiation
- Replaced by additional bits from the randomness source
  - Entropy source: 3/2 (security strength) bits of entropy
  - RBG: bit string 3/2 (security strength() bits long



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!