ANSI X9.82, Part 3
DRBGs

Elaine Barker and John Kelsey
NIST

February 11, 2004

Changes

- Section 7: Functional Requirements modified in accordance with Part 1 changes
  - Removed top-level security requirements (now defined as properties in Part 1)
  - Entropy source → entropy input
- Section 8.2: DRBG Boundary
  - Figures use generic DRBG rather than SHA1_Hash_DRBG

Changes (contd.)

- Section 8.3: Added discussion and figure re the relationship between an instantiation and an instance
- Section 8.4: Seeds
  - Added discussion re seed construction: seed = df (entropy_bits, personalization_string)
  - Seed entropy: entropy ≥ max (128, strength)
  - Seed size: depends on the DRBG

Changes (contd.)

- Section 8.5: Keys
  - Key entropy: entropy ≥ max (128, strength)
  - Removed text re keys from an external source
  - Added text re entropy source for a key (i.e., the seed) and key secrecy
  - Key separation: reworded to account for other changes in the section
- Section 8.7: Prediction and Backtracking Resistance
  - Additional text and a figure for explanation of the concepts
  - Goal: backtracking resistance for all DRBGs

Changes (contd.)

- Section 9.2: Effective security strength, etc.
  - min_entropy = max (128, strength)
- Section 9.4 and 95: Used different examples
- Section 9.6.1: Instantiation call
  - Removed backward secrecy flag, collision flag and seed as input
  - Added prediction resistance capability request flag and personalization string as inputs

Changes (contd.)

- Section 9.7: Reseeding
  - Combined two reseed functions into one function
  - Usage class is only input parameter
- Section 9.8.2: Generating Pseudorandom Bits
  - Removed collision flag and backward secrecy flag
  - Added prediction resistance flag

Changes (contd.)

- Section 9.9: Inserting Additional Entropy Between Requests
  - Added request sufficient entropy and always update flags
- Section 10: DRBG Specifications
  - Removed SHA1_Hash_DRBG (not desirable for new implementations), Keyed_Hash_DRBG (may be replaced) and 3BlockCipher_DRBG (not desirable)
  - New proposed DRBGs being analyzed

Changes (contd.)

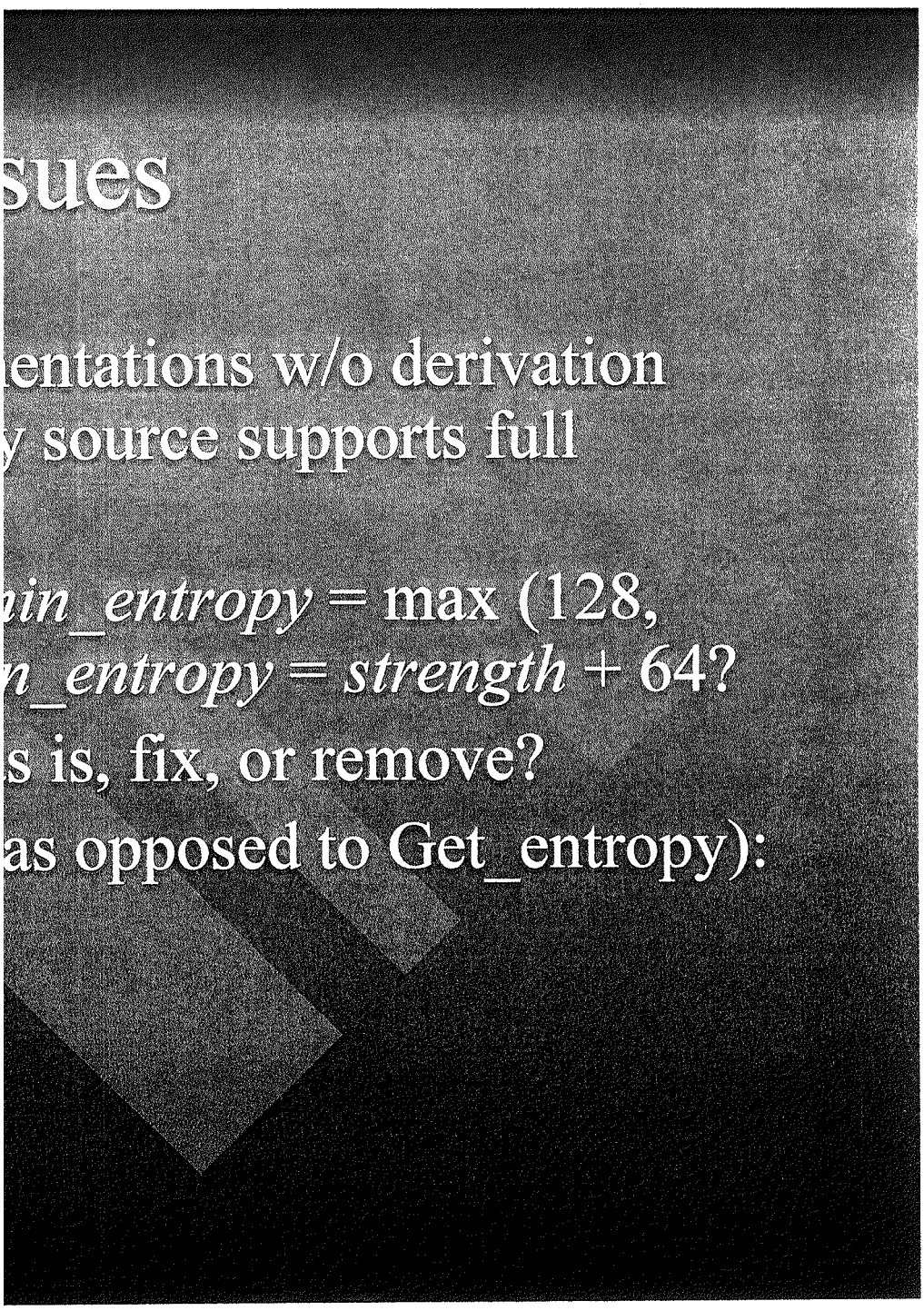
- Section 10.1.2: Hash_DRBG
  - May be replaced or modified; does not provide backtracking resistance
  - Revised to indicate how the personalization string and prediction resistance capability could be used
- Section 10.3.2: Dual_EC_DRBG
  - New specifications
  - To be done: revise method of using the prediction resistance capability; use personalization string

Changes (contd.)

- Section 10.3.3: msDRBG
  - DRBG specified like other DRBGs
  - To be done: revise method of using the prediction resistance capability; use personalization string

Iss

- Allow DRBGs implem
  functions when entropy
  entropy?
- Instantiation: require *m*
  strength) or require *mi*
- Hash_DRBG: Retain a
- Get_additional_input (
  - Purpose?
  - Entropy requirement?
  - Personalization?


sues
entations w/o derivation
y source supports full
in_entropy = max (128,
n_entropy = strength + 64?
s is, fix, or remove?
as opposed to Get_entropy):

Schedule

- Next draft available early to mid May?
- Written comments by late May?
- Discussion at Toronto Meeting (June 8-11)
- RNG Workshop at NIST (July 19-22)
  - Post draft standard by late June?