Randomness Beacon Applications

Interoperable Randomness Beacons, Cryptographic Technology Group, Computer Security Division

INFORMATION TECHNOLOGY LABORATORY

NIST National Institute of Standards and Technology U.S. Department of Commerce

Public randomness

A useful resource for the public good. A beacon *pulsates* randomness with challenging features:

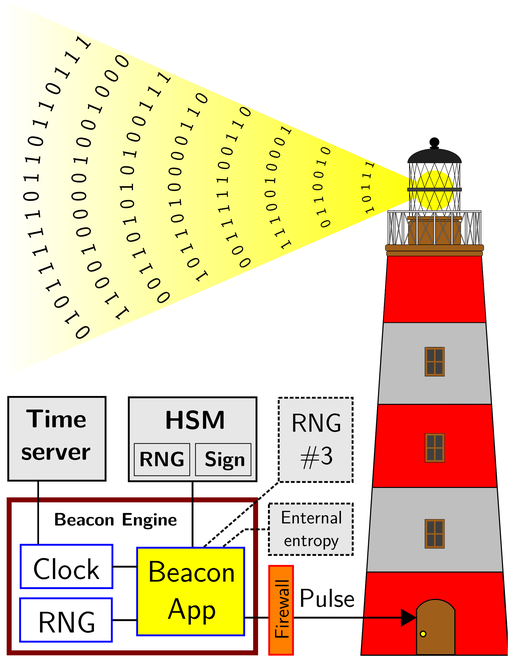
- **Fresh:** Produced when it is claimed.
- **Unpredictable:** No one can predict its value.
- **Unbiased:** No influenced property (e.g., last bit).
- **Consistent:** Timely and available forever.
- **Interoperable:** Combinable with others.

A curious duality: To ensure **public auditability**, one promises to use **randomness** (public) from future time t, as input to a **deterministic** algorithm A, to obtain choices C.

Get your fresh dose of public randomness:

Poster produced by Luís T. A. N. Brandão (at NIST as Contractor from Strativia) and presented by Harold Booth at the NIST-ITL Science Day 2021 (October 28). More info at https://csrc.nist.gov/projects/Interoperable-Randomness-Beacons

NIST Rand. Beacon



Miscellaneous facts:

- More than 1.5M pulses since chain #2 started on 2018-Jul-23.
- Includes a quantum random bit generator built by NIST-PML.
- U.S., Chile and Brazil have beacons following the NIST reference (IR 8213)

Conceived applications

- **Clinical trials.** The public can check the trial was properly randomized.
- **Legal Metrology.** Ensure fresh proofs of software possession by measuring instruments.
- **Financial Audits.** Select public official for audit, without risk of political biasing.
- **Judge selection.** Defenders and prosecutors verify unbiased choice of judge to court case.
- **Quality control.** Build audit trail for later verification of the selected sample.

Future looking forward

- Guidance for applications with public-auditability
- Open source code to facilitate other deployments
- External values for better freshness verifiability
- Enhanced crypto (threshold, post-quantum, ...)