The NIST Randomness Beacon 2.0

Lawrence Bassham, Harold Booth, Luís Brandão, John Kelsey, René Peralta

Cryptographic Technology Group, Computer Security Division, ITL, NIST

The NIST Randomness Beacon

- Broadcasts a randomness **pulse** every 60 seconds
- Each pulse commits to a fresh 512-bit random string
- Each pulse is time-stamped and signed by NIST
- Hash-chained pulses create an immutable public record
- Cryptographic fields support strong trust assurance

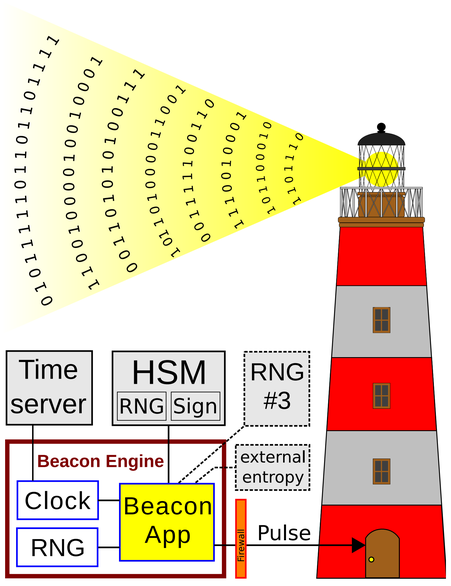


Figure 1: Clipart depiction of the beacon components

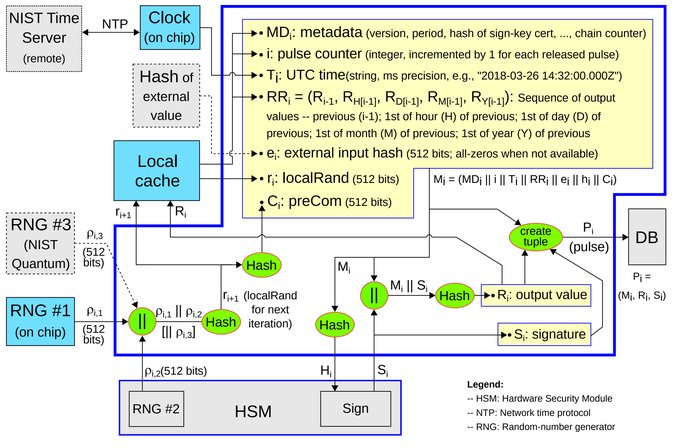


Figure 2: Generation of the *i*-th pulse in the NIST Beacon App version 2

Public randomness

A common source of randomness can be useful in many situations

We often agree that the best way to pick is at random (lotteries, audits, quality control,...), but it is difficult to do this when the parties are many and/or cannot be assembled in one place. A public source of trusted randomness like the NIST Beacon solves this problem.

- The first prototype of the NIST Beacon was deployed in 2013
- In 2018, NIST deployed version 2 of the Beacon service
- Draft NISTIR 8213 specifies the new Beacon format
- Development of applications is a matter of ongoing research

Example: placebo-controlled trials

A placebo-controlled clinical trial assigns patients to either the treatment group or the control group.

After the study, it may become necessary to convince others that the trial was properly randomized.

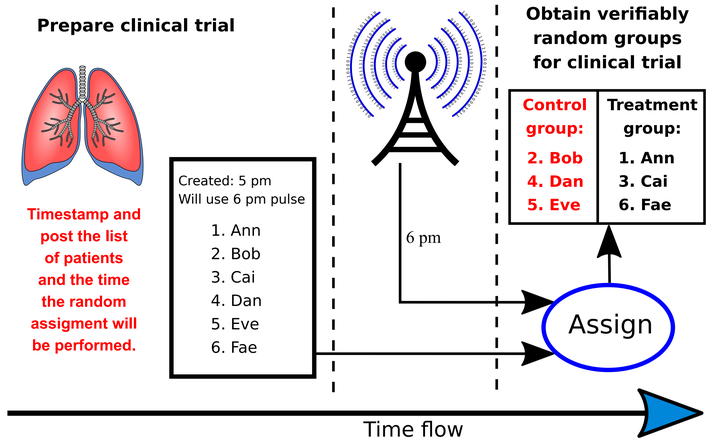


Figure 3: Time flow of clinical trial protected by the Beacon

Example: auditing a politician

Problem: How do you convince a politician that he or she was randomly chosen for a tax audit?

Solution: use the NIST Beacon.

Potential applications

- Randomizing the selection of government officials for financial audits
- Enabling verifiable sampling for lot quality assurance
- Assigning court cases to random judges
- Thwarting protectionist measures hidden in import inspection regimes
- Preventing gaming of cleanliness inspection regimes in hospitals
- Replacing costly proof-of-work mechanisms in crypto-currencies
- Time-bracketing video evidence usable in a court of law

Interoperability across beacons

The new Beacon format (2.0) provides the ability to combine randomness from different beacons. Any good beacon is enough to ensure good combined randomness, thus reducing trust requirements.

Several randomness beacons are being developed:

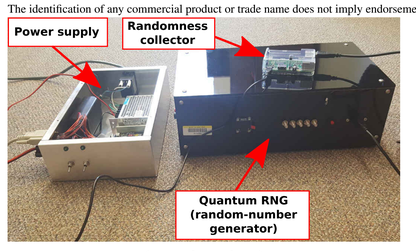
- (United States) NIST Randomness Beacon https://beacon.nist.gov/home
- (Chile) CLCERT Randomness Beacon https://beacon.clcert.cl/
- (Brazil) Brazilian Randomness Beacon beacon.inmetro.gov.br:8090

Figure 4: Countries developing Randomness beacons interoperable with NIST

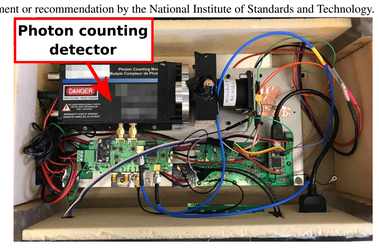
Randomness sources

The randomness of a Beacon must result from the combination of at least two certified sources of cryptographic randomness. The NIST Randomness Beacon will incorporate a third source, using randomness obtained from a quantum process related to probabilistic detection of photons. The device was developed by Joshua Bienfang and Michael Wayne's team at the NIST's Physical Measurement Laboratory, which also participates in the NIST Randomness project.

The identification of any commercial product or trade name does not imply endorsement or recommendation by the National Institute of Standards and Technology.



(exterior view)



(interior view)

Figure 5: Quantum RNG device

Example: `localRandomValue` at `2018-10-01T00:00:00.000Z` (UTC): `1CD91A7B1F8E8A452BC8A20609A2026AB46D20DC59B51C11F97A729B180A2A3E790B68DC7C89DC001658C15FC8644BF494F2416B2E9226044584CECA11BA90CE`

Poster produced for the NIST-ITL Science Day 2018 — November 01, 2018 (Gaithersburg MD, USA)