THE NIST RANDOMNESS BEACON

Rene Peralta

Computer Security Division
National Institute of Standards and Technology.

What this is not

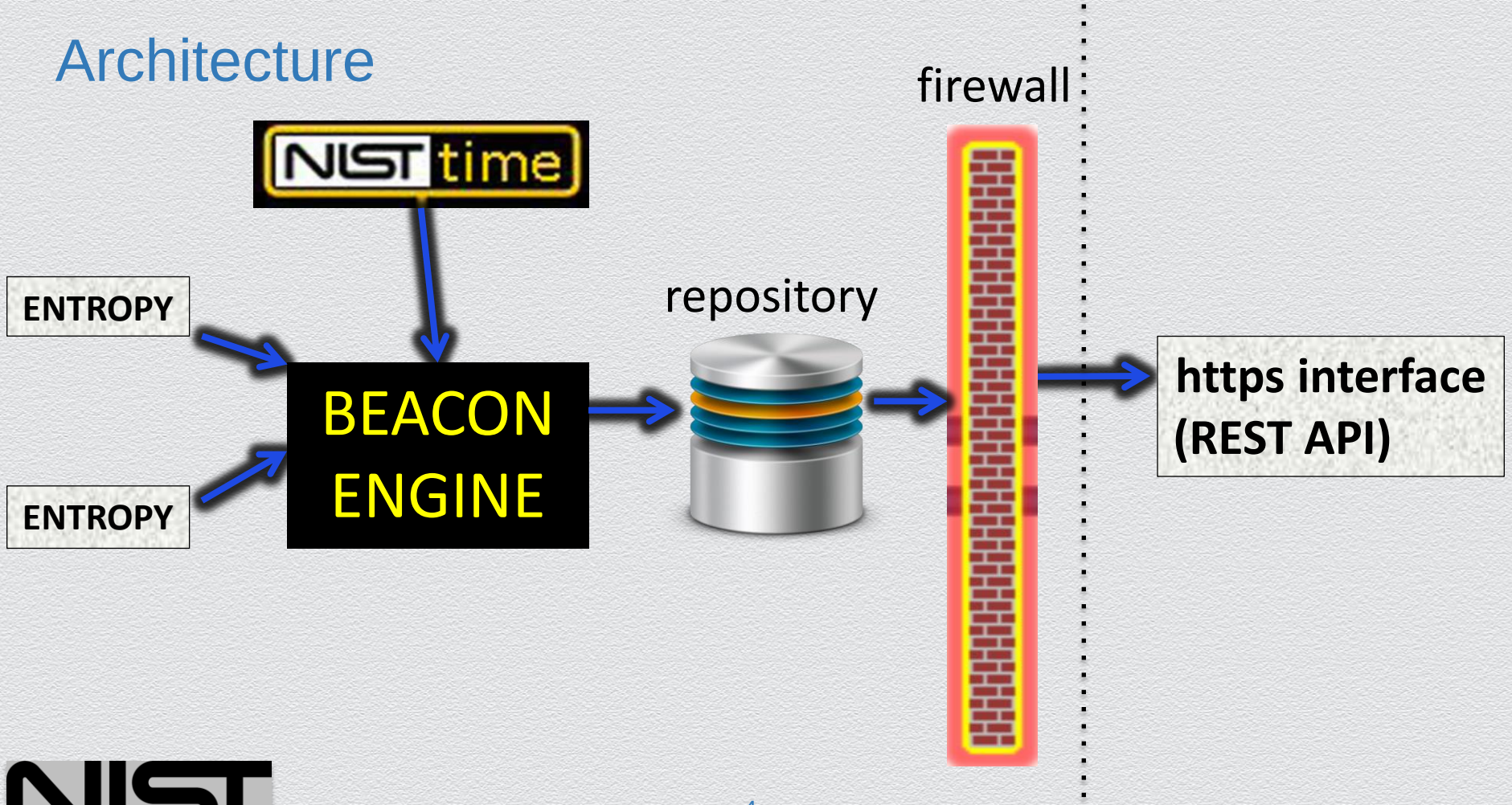
This is not for generation of secret keys.

What this is

- Public randomness
- publish model
- digitally signed and time-stamped

- https://beacon.nist.gov/home

Architecture



Motivation

- Public, time-bound randomness is a valuable resource

- A standard for such a resource is needed so that it can be replicated by other institutions

Properties

- Unpredictability
- Autonomy
- Consistency
- “Forever” unforgeable public record

Sample applications

- Provably random sampling
- Selective disclosures. An important goal of NSTIC

Selective Disclosure Scenario

- You carry authenticated and encrypted data about yourself on a smart card

DATA

You have 

- A function of this data is required for a given transaction (e.g.

  F(DATA) = “over 21 or doctor authorization to obtain <medication>”)

Can you trust it?

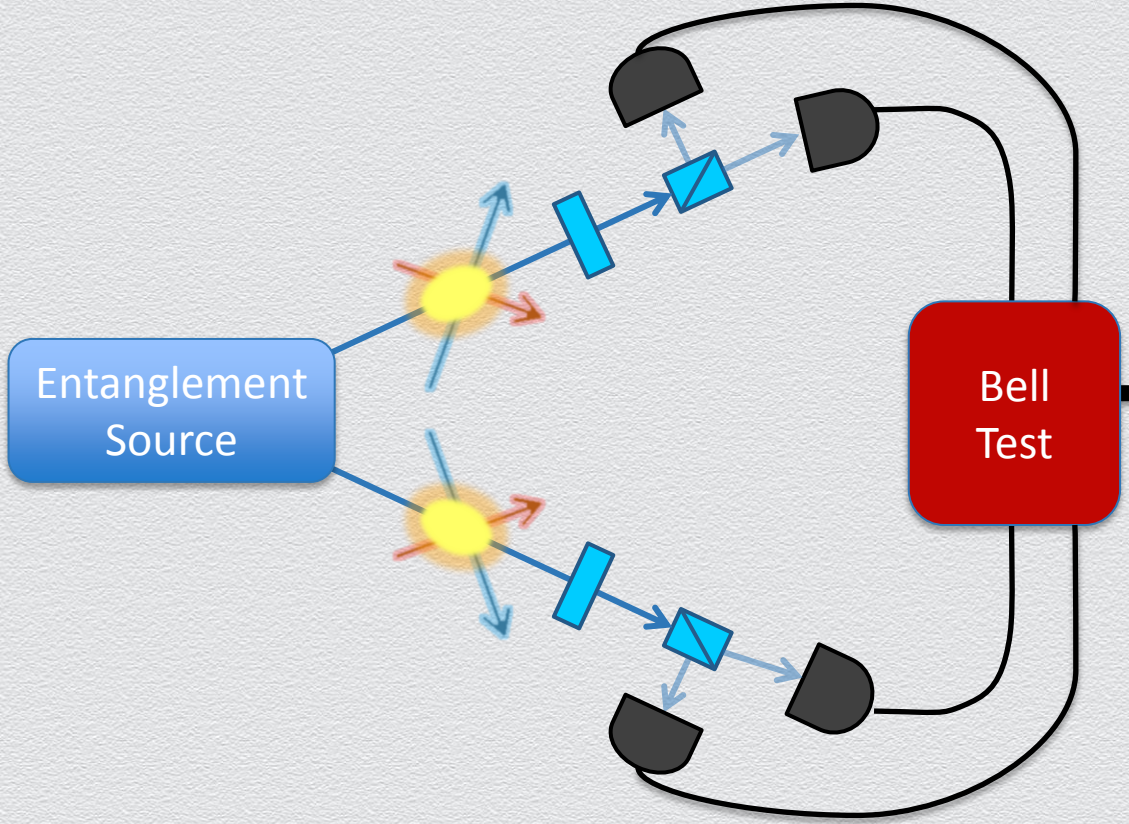
- You don’t have to!
  - can be combined with other sources
  - a “cooked” number could only target one application
  - historical record is robust against tampering, even by NIST

Entropy

- Currently using two independent commercial RNGs

- We plan to implement a “verifiable source”. This is a collaborative project between NIST’s Information Technology and Physical Measurement laboratories.

Verifiable quantum randomness source



Output uncorrelated with anything outside the apparatus.

The bigger picture

- We view this as a type of “trust anchor” for the Internet
  - something that is hard to subvert for gain
  - a primitive that can be leveraged for many purposes

- We hope it will encourage other such “anchors”

Summary

- We are enabling “verifiably random” sampling
- The are simplifying existing digital interactions and enabling new ones
- We are developing the best randomness source in the world
- Project page at
  http://www.nist.gov/itl/csd/ct/nist_beacon.cfm

Sharing is the way to go

THANK YOU

Interactive proofs

DATA