Low-Cost Threshold Cryptography HSM for OpenDNSSEC

Francisco Cifuentes
francisco@niclabs.cl

Problem description

- To satisfy security needs, DNS operators use Hardware Security Modules.
- Specialized hardware that have special security properties.
  - http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Problem description

- HSM are **expensive.**
  - $50 - $50000
  - FIPS 140-2 level 1 to level 4.
  - High security level implies high price.
- Small institutions want to deploy DNSSEC but they can not buy them.

Problem description

- What if ...
  - we could achieve a good security level without paying that much?
  - we use old and not in use hardware, and we achieve a good security level not paying at all...

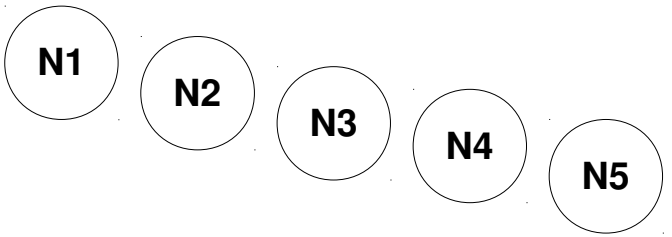
Proposed solution:

Low-Cost Threshold Cryptography HSM for OpenDNSSEC

Francisco Cifuentes
francisco@niclabs.cl

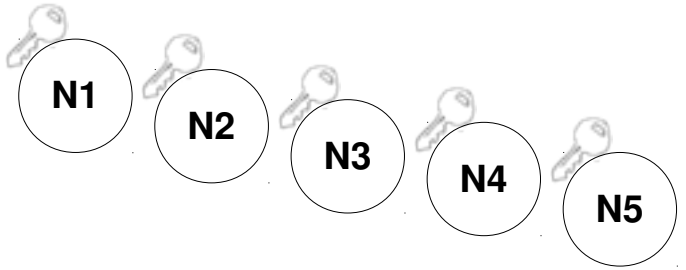
Solution description

- Threshold Cryptography



Solution description

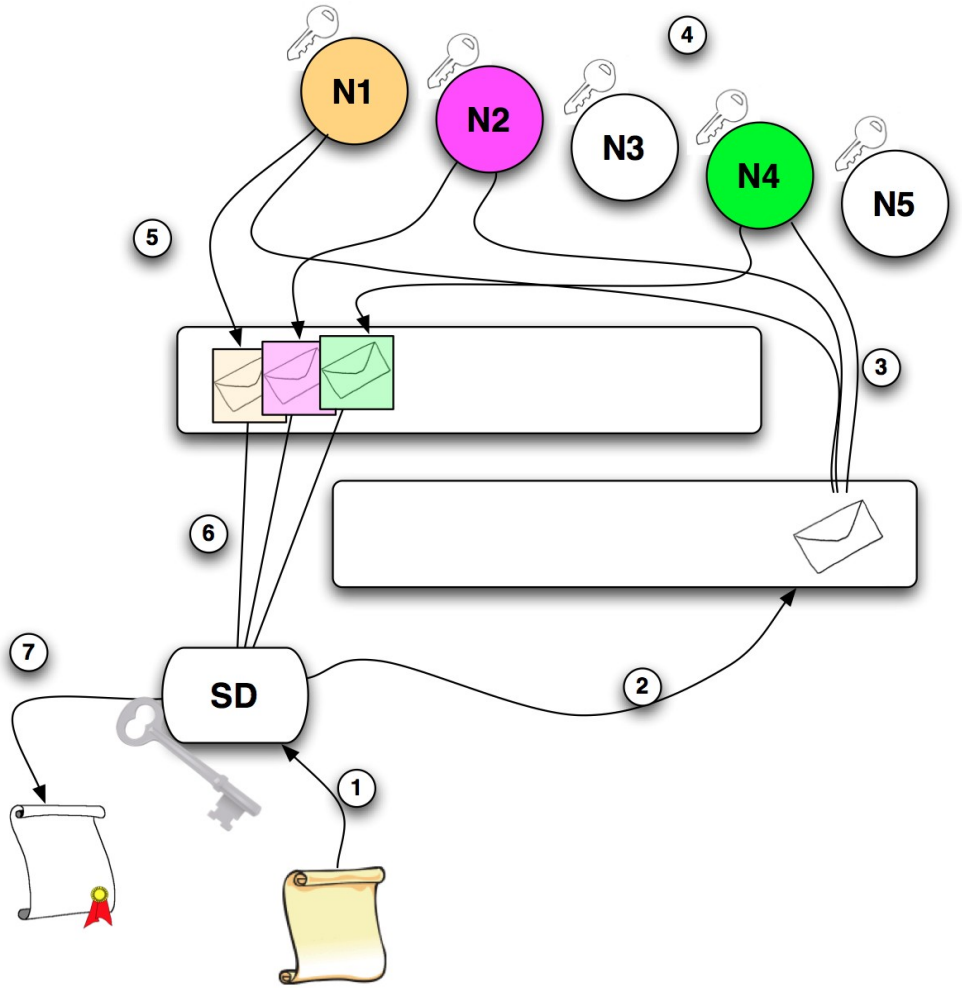
- Threshold Cryptography



SD

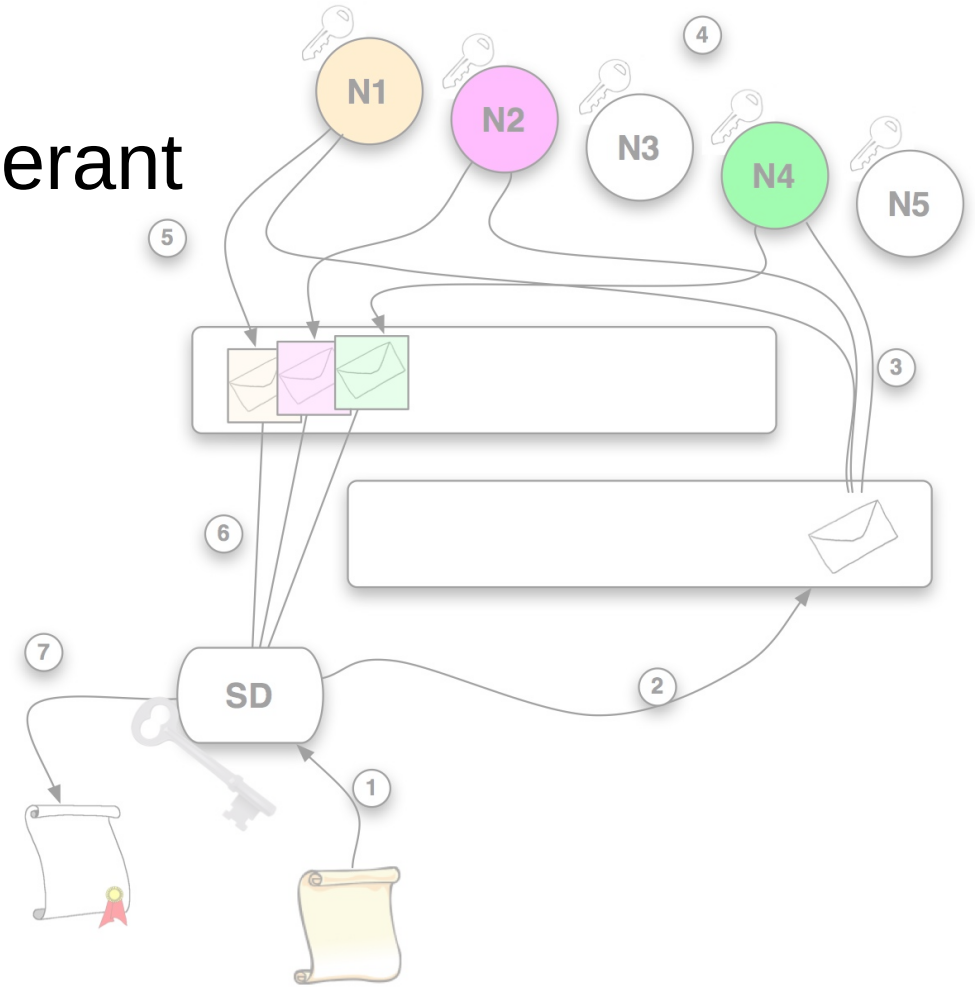
Solution description

- Threshold Cryptography



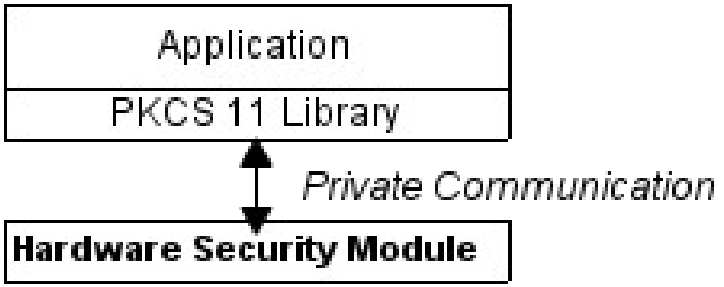
Solution description

- Threshold Cryptography:
  - Secure
  - Fault tolerant
  - Robust



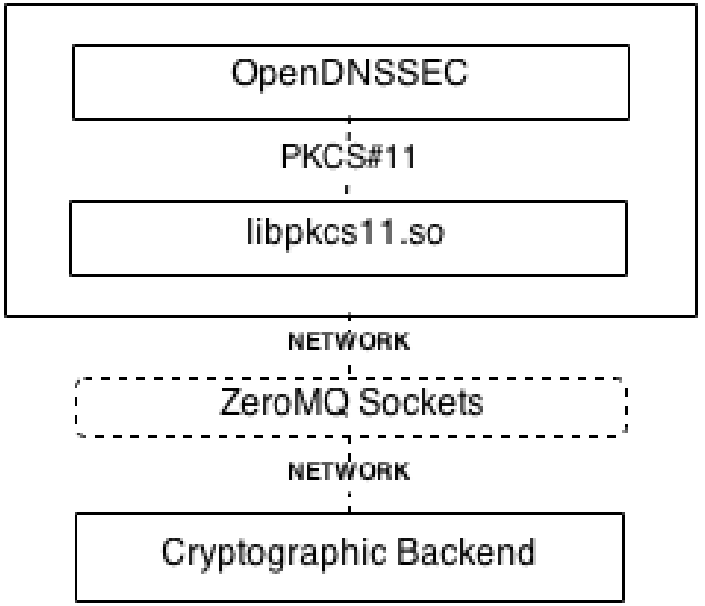
Solution description

- HSM basic architecture



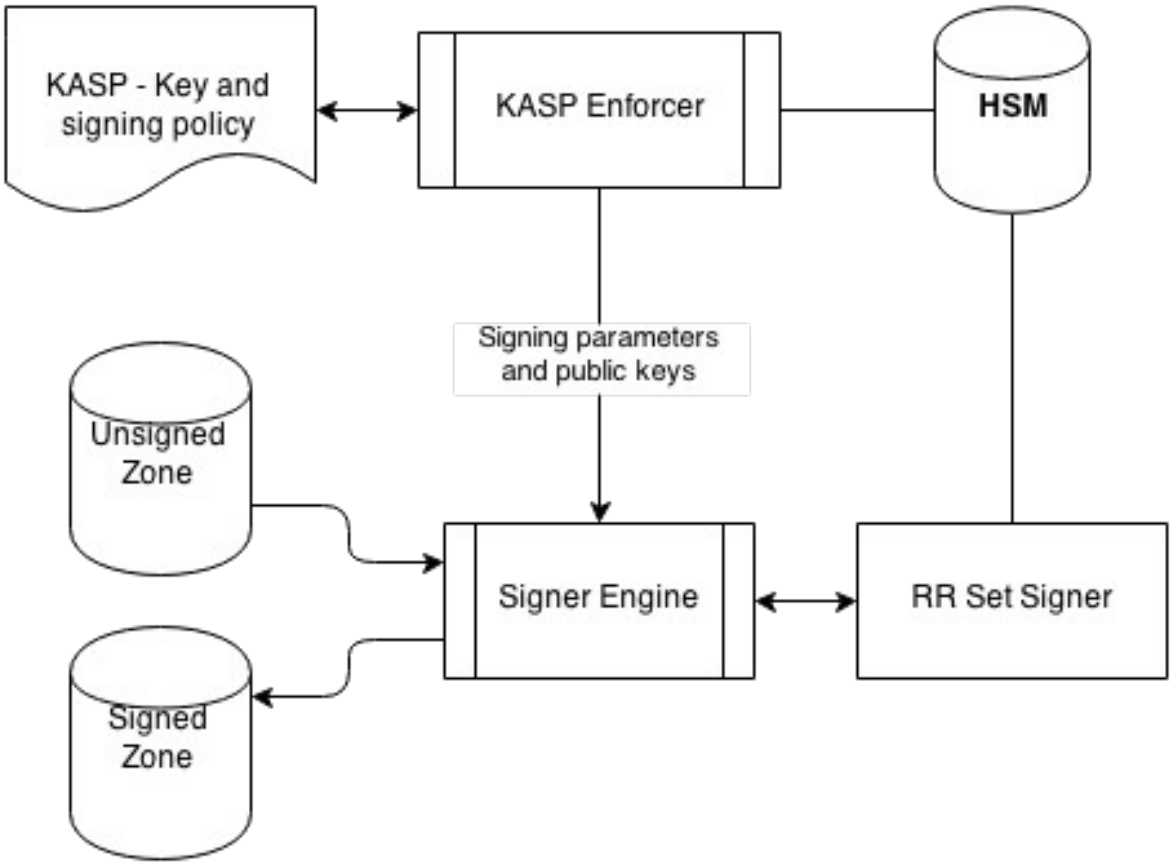
Solution description

- TCHSM Architecture



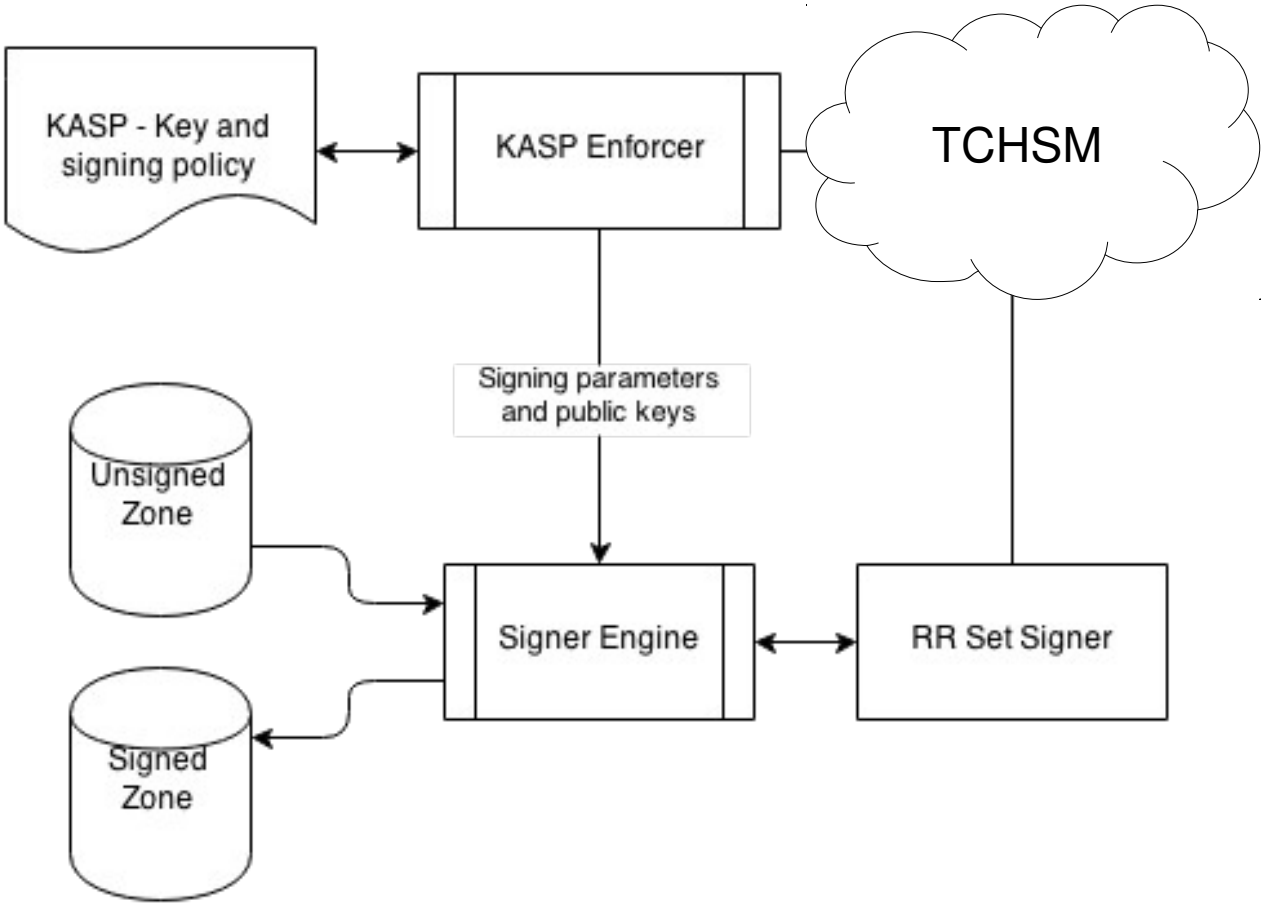
Solution description

OpenDNSSEC Architecture

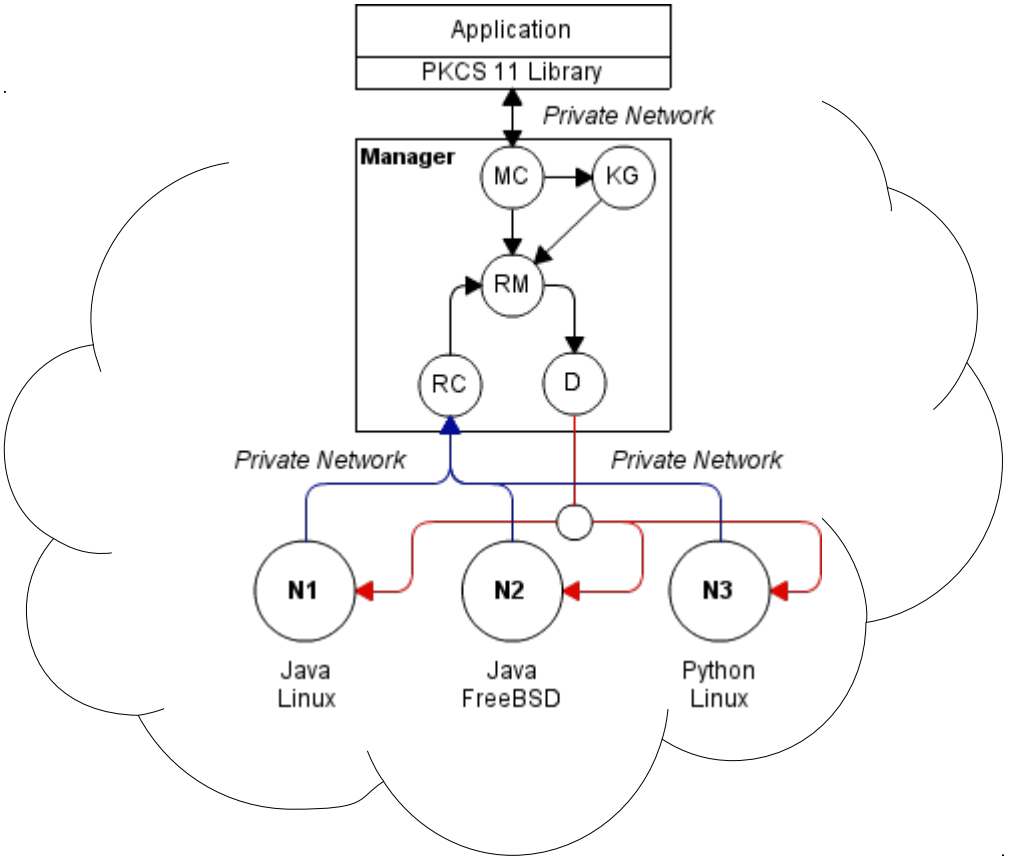


Solution description

OpenDNSSEC Architecture



Solution description

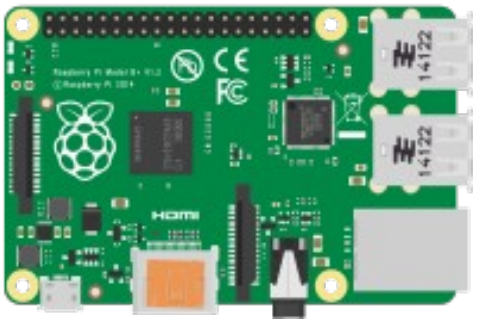


Experiments and results

2 Configuration

- Typical desktop computer
- Intel dual-core processors at 2.8 GHz
- 4 MB of memory cache and 1 GB of RAM
- (one of them used as DNS server with OpenDNSSEC)

- Raspberry PI
- Broadcom BCM2835 ARM unicore at 700 MHz, 128 KB of memory cache
- 512 MB RAM



Gigabit LAN with latency lower than 1 second, 8 machines of the same type connected.

Our Raspberry PI Cluster!

Experiments and results

Experiment

- 8 nodes try to sign the zone registry.
- The signature dealer waits until the first 5 not compromised nodes sign the zone registry.
- Measuring the average time of the generation of 1000 RRSIG signatures.
- Also measuring the average time of the generation of 1000 RRSIG signatures using the SoftHSM solution made by OpenDNSSEC's developers.

Experiments and results

Results

Key Size	1024 bits		2048 bits		Project Cost
	SoftHSM	TCHSM	SoftHSM	TCHSM	
Desktop PC	5 ms	69 ms	14 ms	283 ms	$0†
Raspberry PI	21 ms	382 ms	81 ms	1408 ms	$35 x 8 = $280

† **We use old computers that were not in use :-)**

Implementation problems

- Managed systems memory zeroization.

Future Work

- Implementation diversity.
- Full distributed threshold RSA.
- GPU Usage.
- Replication / Migration.

Distributed HSM

Francisco Cifuentes - francisco@niclabs.cl

Links:

- www.niclabs.cl
- github.com/niclabs/tscrypto