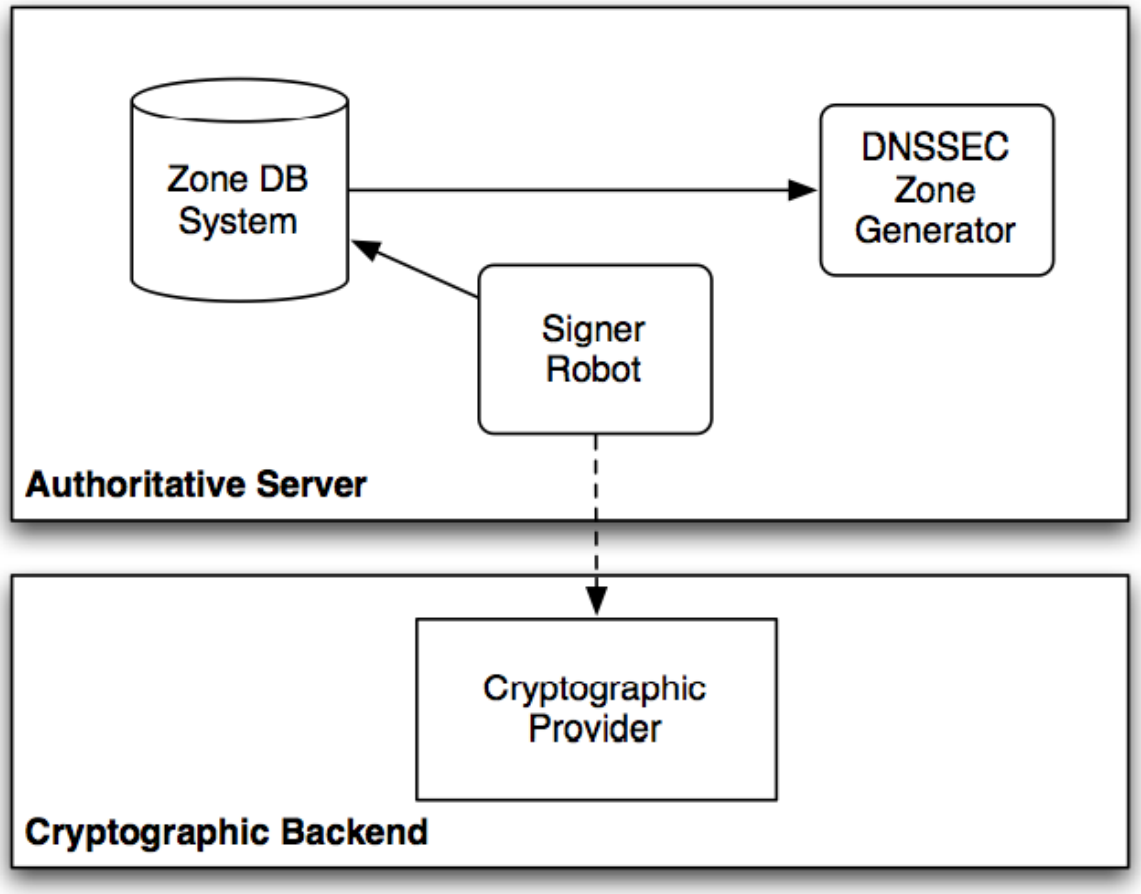
A Threshold Cryptographic Backend for DNSSEC

Francisco Cifuentes
francisco@niclabs.cl

NIC CHILE Research labs

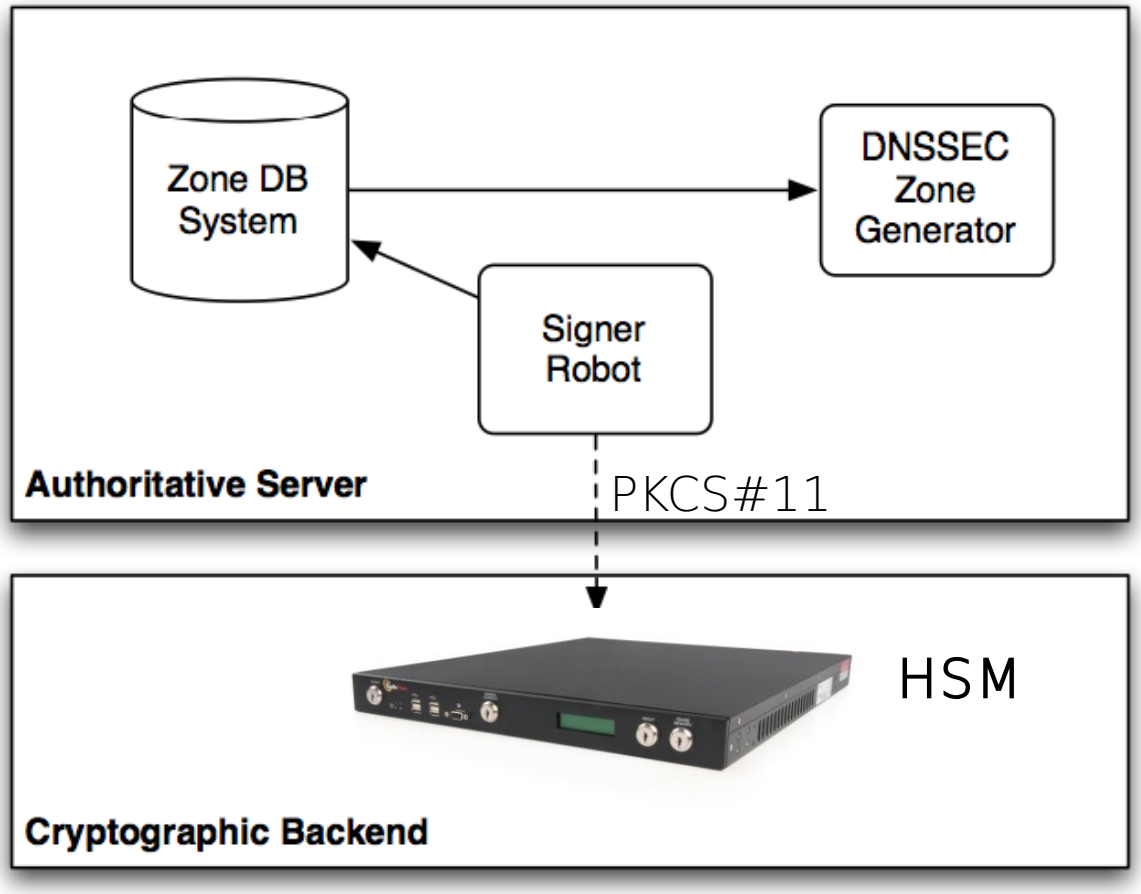
Key Management Implementations

Back to ICANN 40



NIC CHILE Research labs

Key Management Implementations



Needs

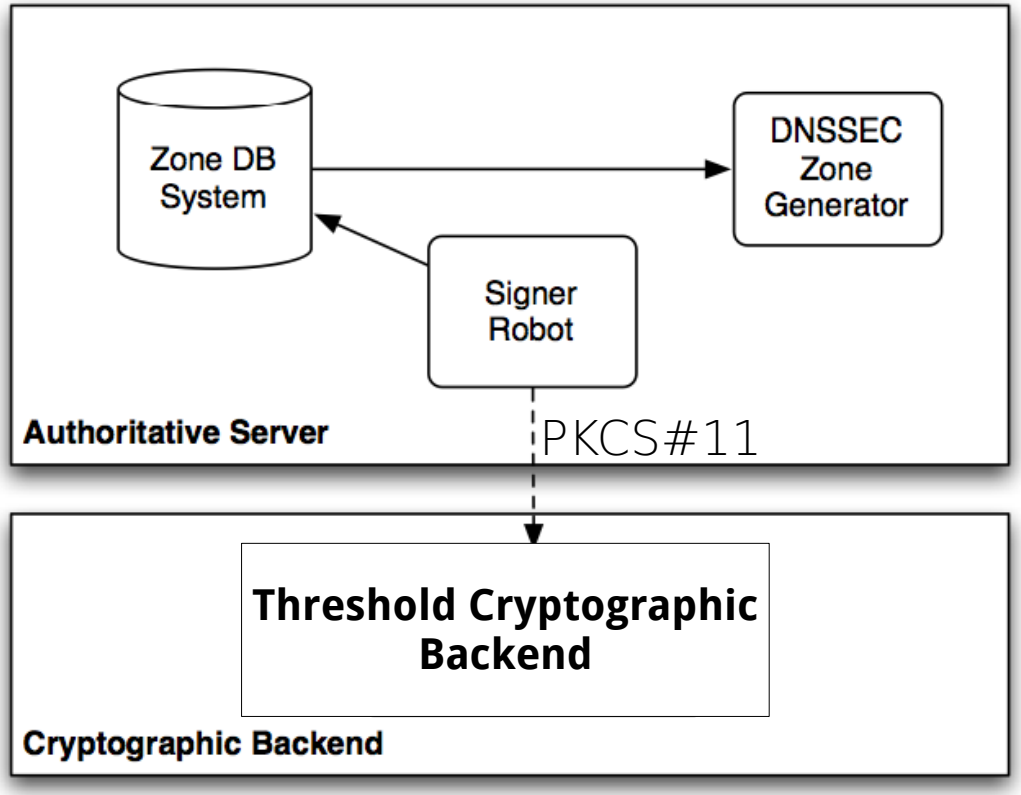
- Zones need to be re-signed periodically.
- Keys must not be cloned.

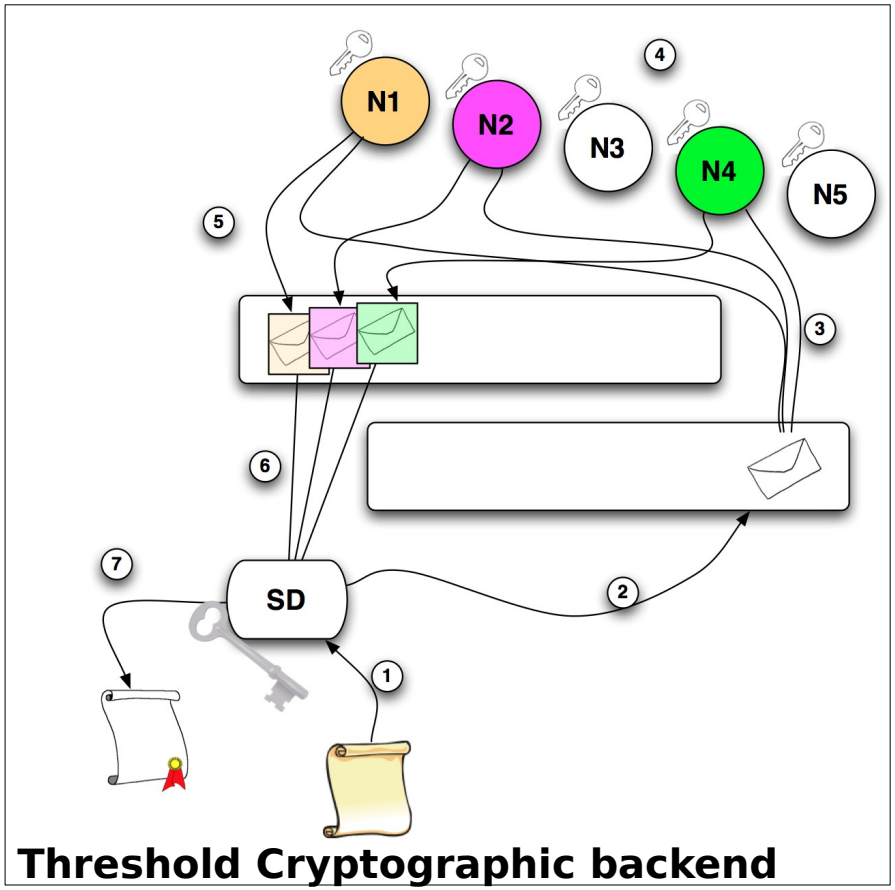
Problems

- Hardware fails.
- HSM are expensive.
- SoftHSM can be vulnerable.

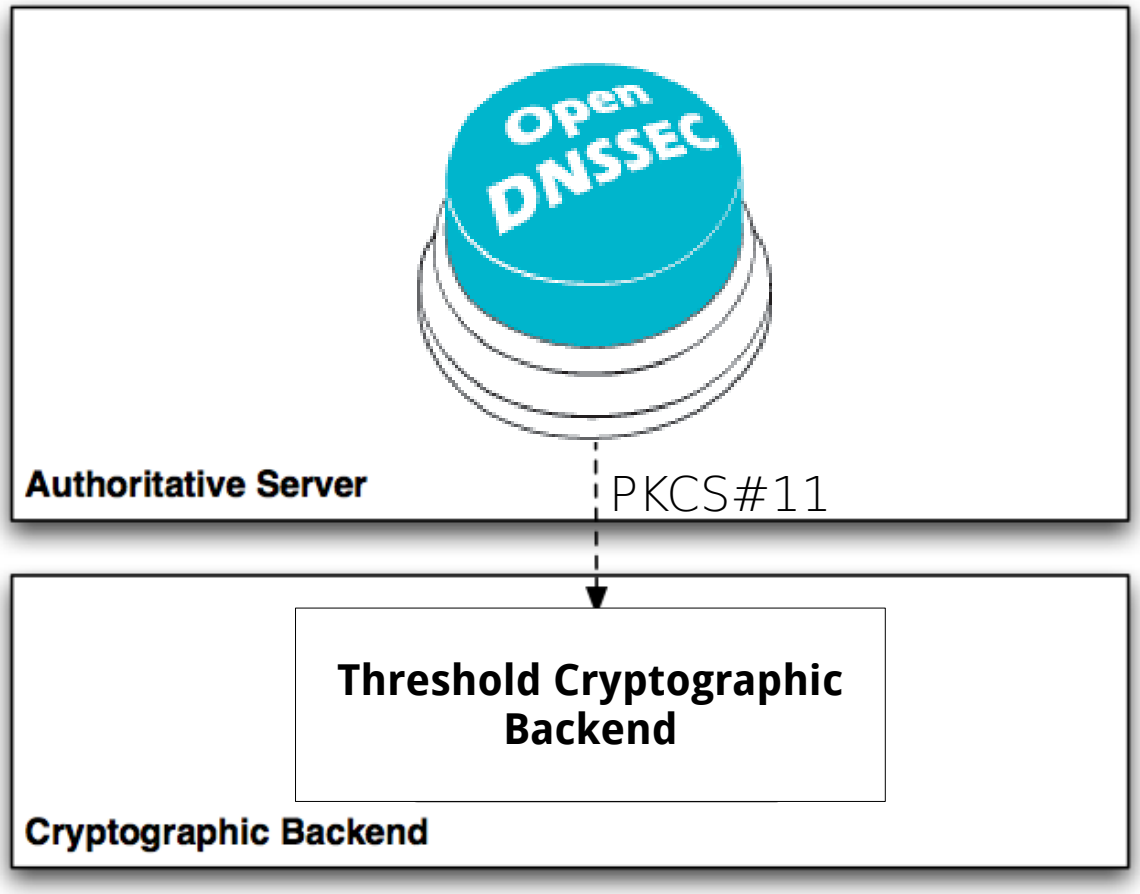
NIC CHILE Research labs

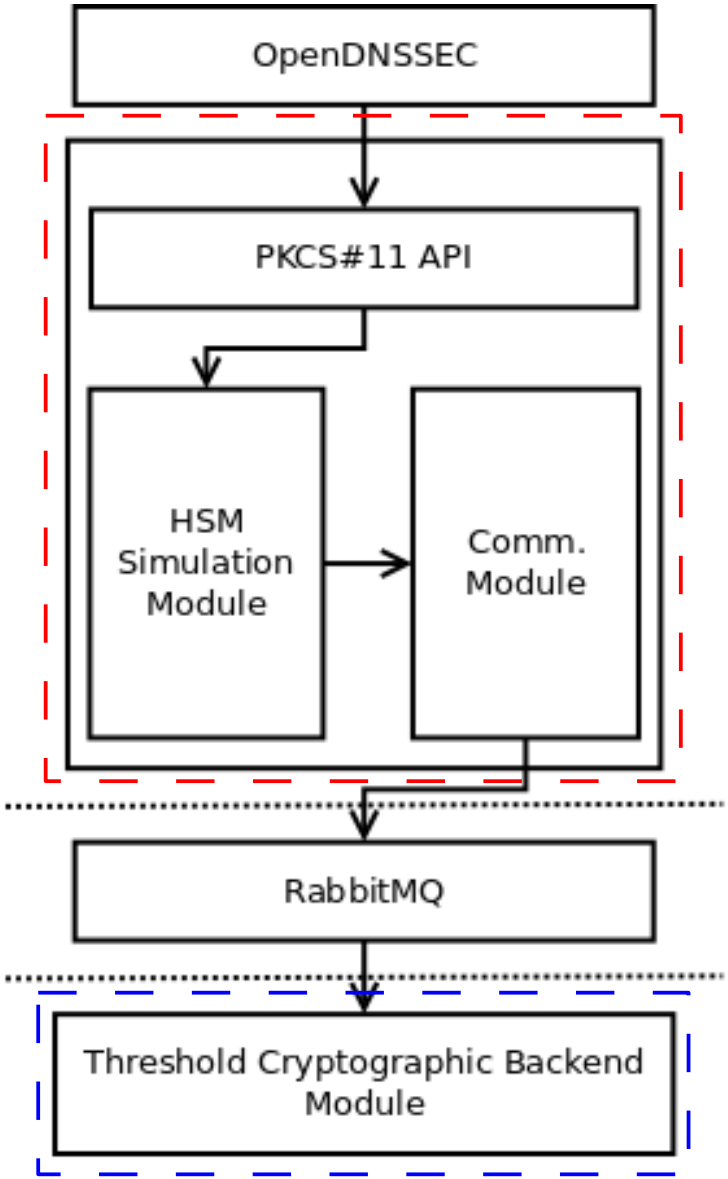
What was proposed?
A Threshold Cryptographic Backend.





Our work with OpenDNSSEC

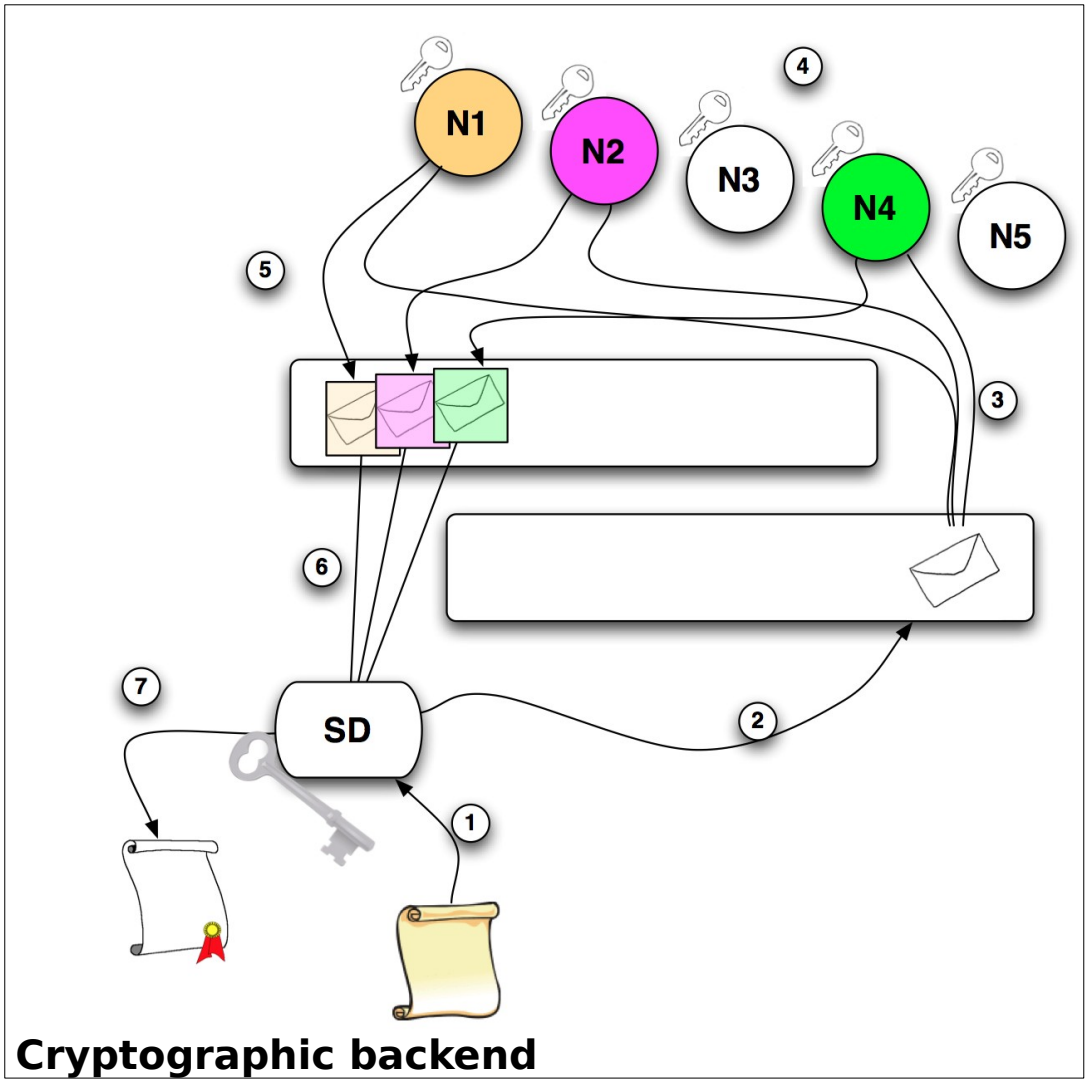




NIC CHILE Research labs

Properties of the system

- Distributed
- Fault Tolerant
- Robust
- Secure

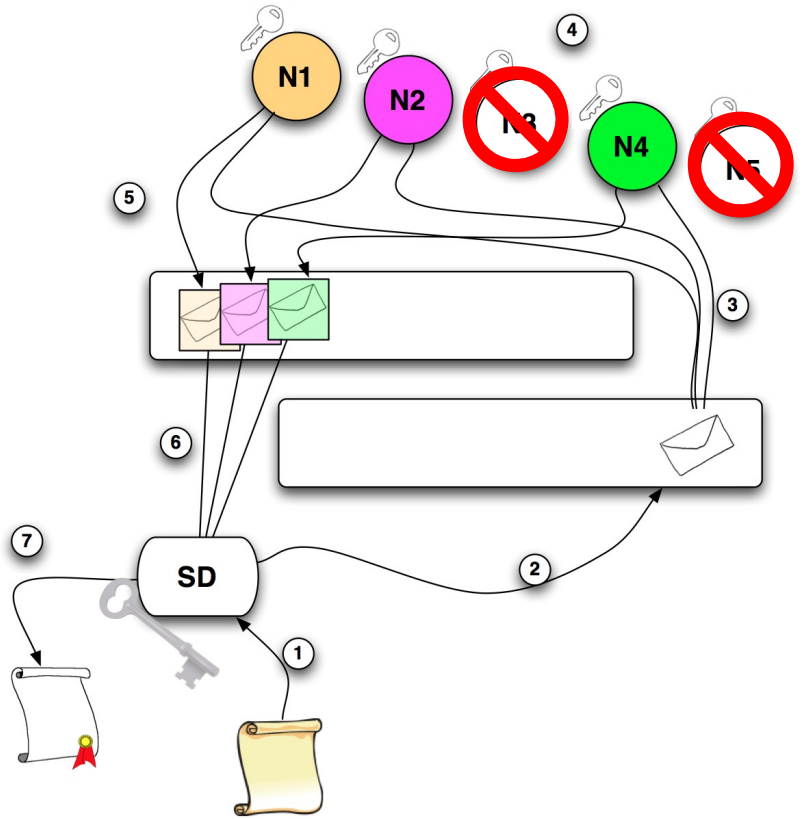


Properties of the system

- Distributed
  - Private key is split into shares and distributed among *n* nodes.
  - The signing procedure is called in each of the *n* nodes.

Properties of the system

- Fault-Tolerant
  - A subset of nodes can fail and the signing process will be completed succesfully.



Properties of the system

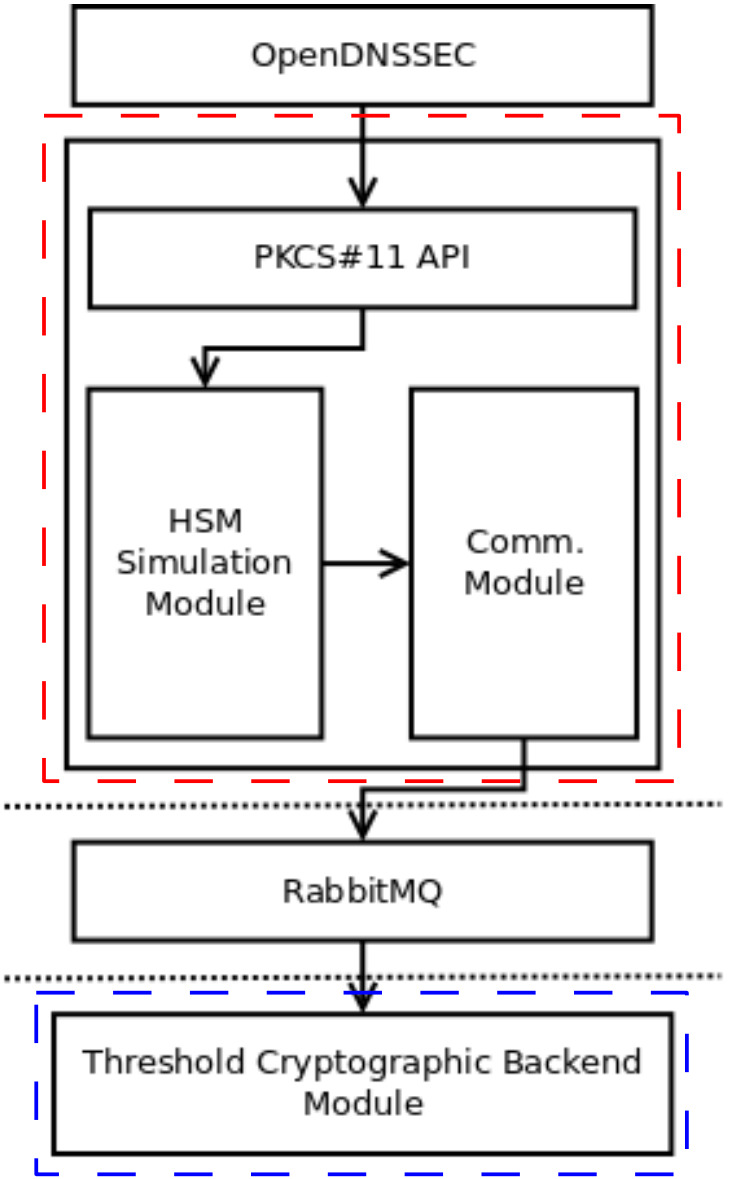
- Robust
  - Failures and attacks can be reduced implementing nodes in both different programming languages and operative systems.

Properties of the system

- Secure
  - No one holds the complete private key.
  - More than *k* nodes have to be endangered to authorize faked signatures.

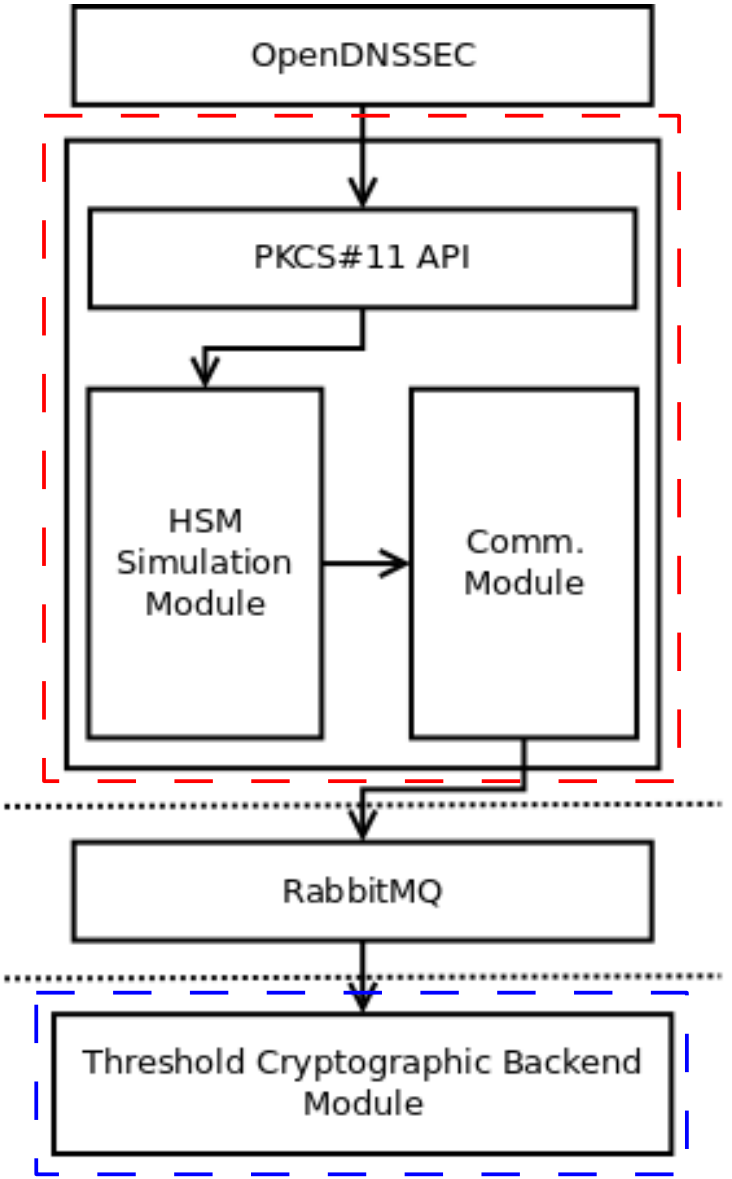
What it is?

- Basically, a PKCS#11 API provider.
- It uses the Threshold Cryptographic Backend implemented then.
- It actually signs DNS records.



What it is not?

- A fully compliant PKCS#11 implementation.



Future work

- Complete the PKCS#11 implementation, in order to make it usable directly from BIND (or any other software).
- Test on a real zone set.

Questions?

Francisco Cifuentes
francisco@niclabs.cl

NIC CHILE Research labs