(Towards) a Threshold Cryptographic Backend for DNSSEC

OARC 2011

Antonio Cansado acansado@niclabs.cl

Pablo Sepúlveda psepulv@niclabs.cl

Tomás Barros tbarros@niclabs.cl

Victor Ramiro vramiro@niclabs.cl

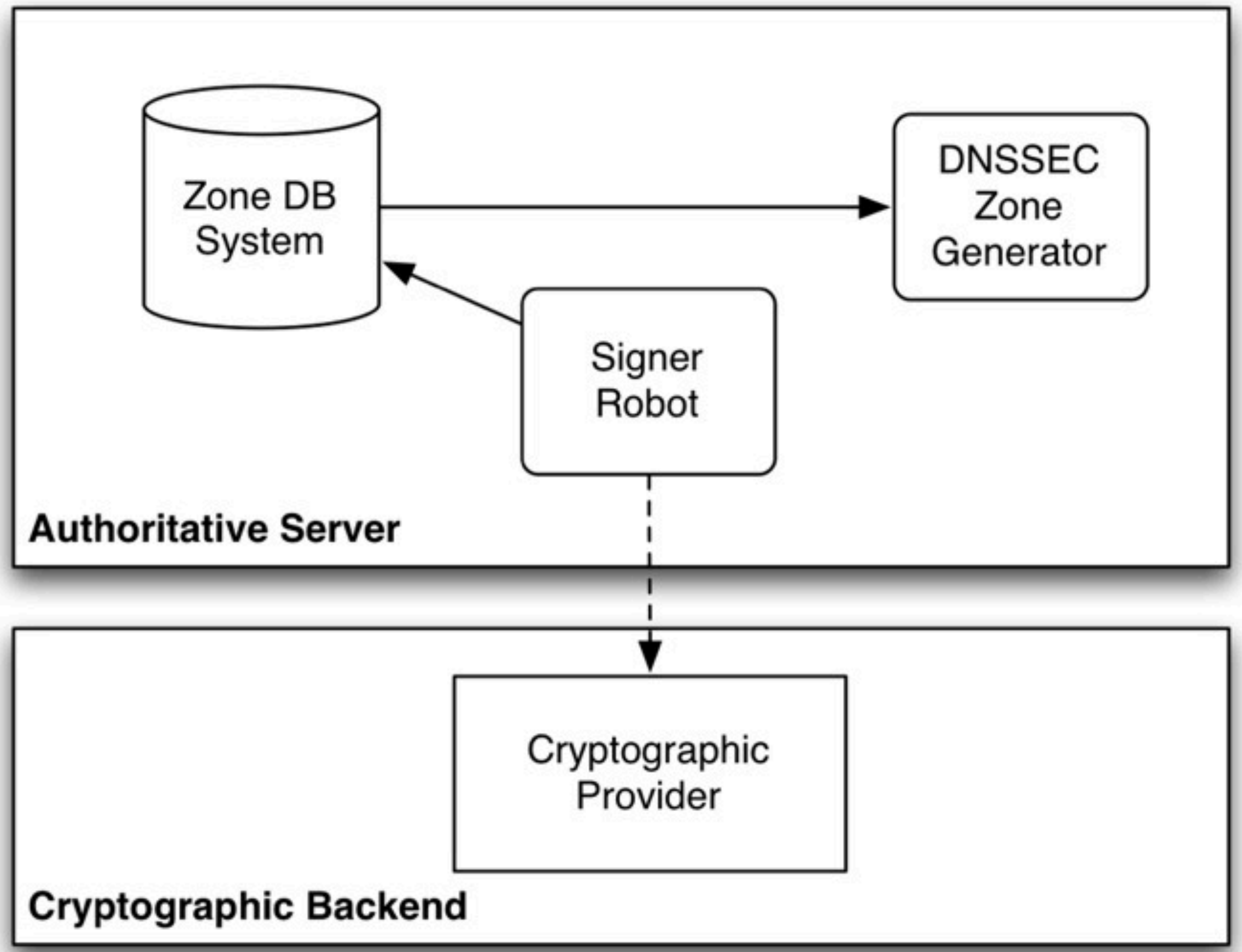
Who are we?

NIC Chile Research Labs is an Applied Research and Technology Transfer Laboratory, founded by NIC Chile (the Chilean ccTLD) on 2008.

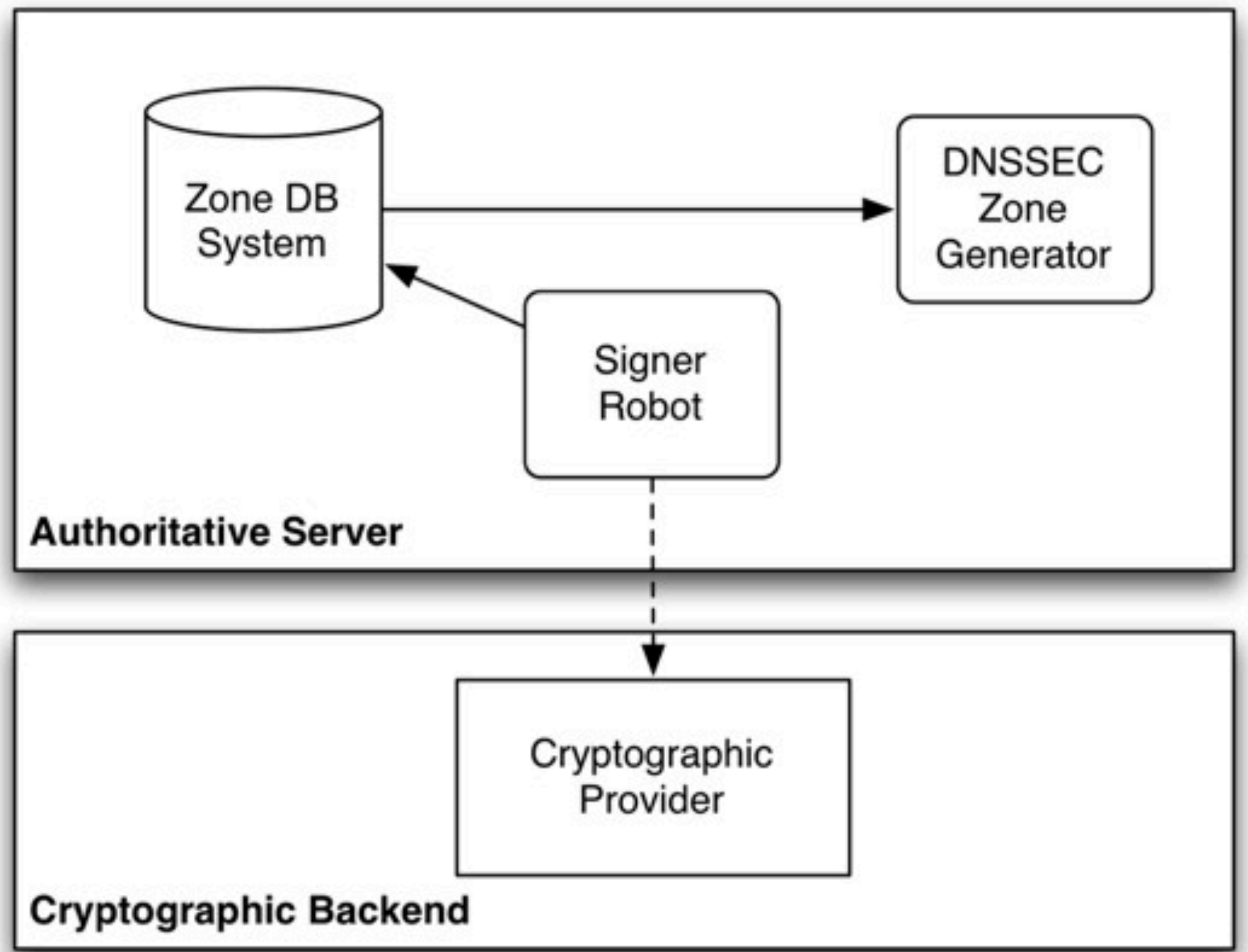
Our Mission: To develop world class research on Internet domain, targeting technology transfer for the regional industry

More info: http://www.niclabs.cl

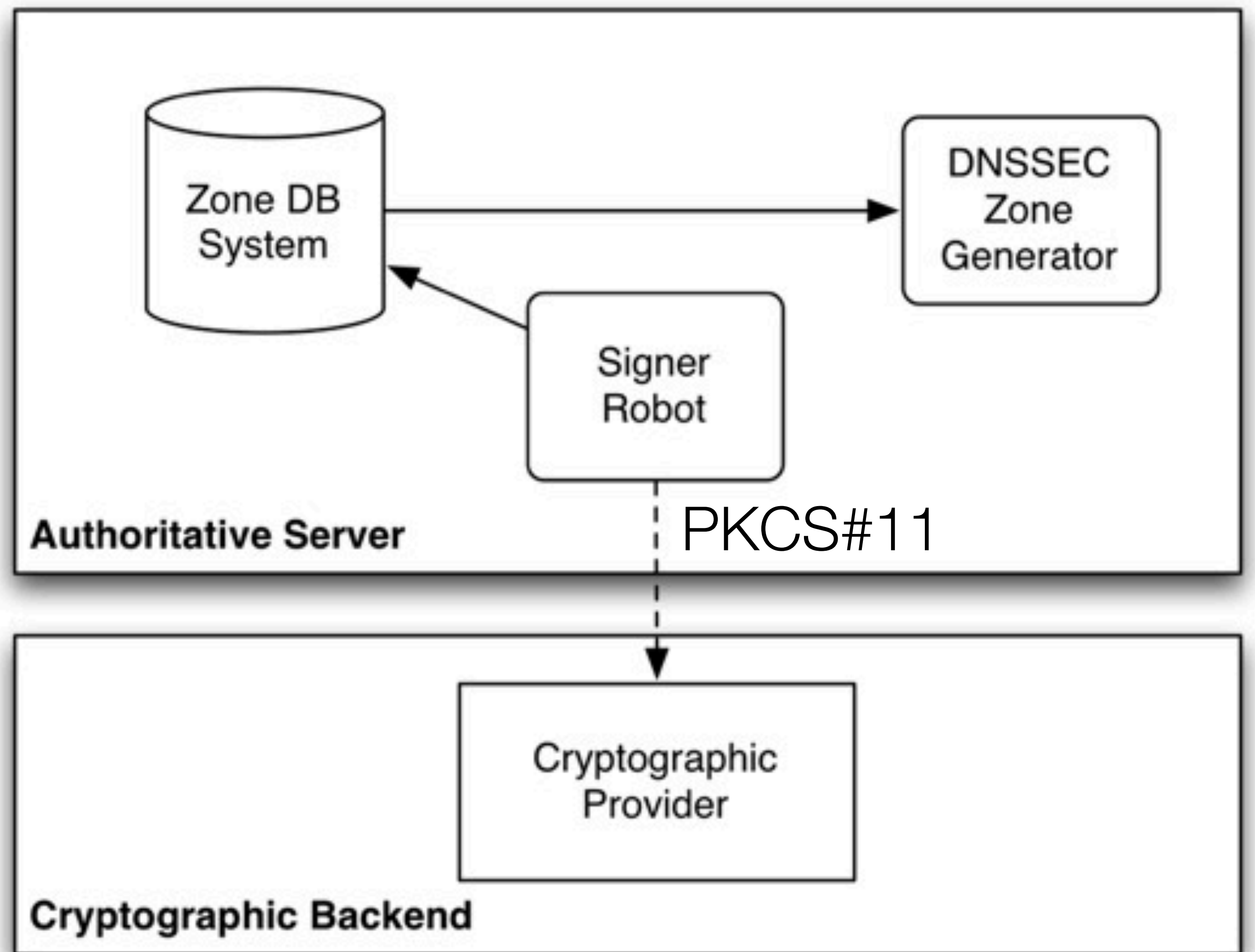
DNSSEC Architecture



DNSSEC Implementations

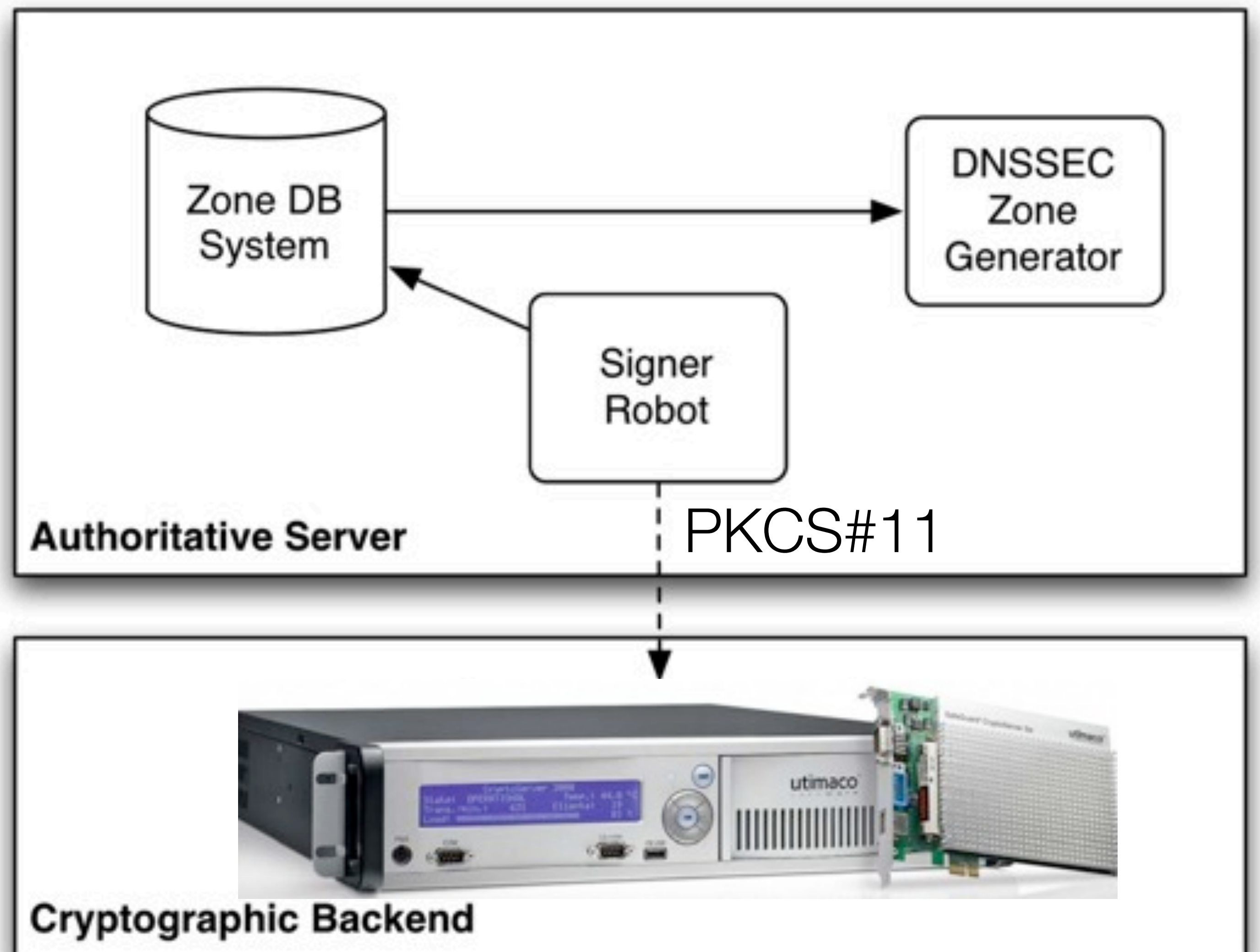


DNSSEC Implementations



Zones need to be re-signed periodically.

DNSSEC Implementations

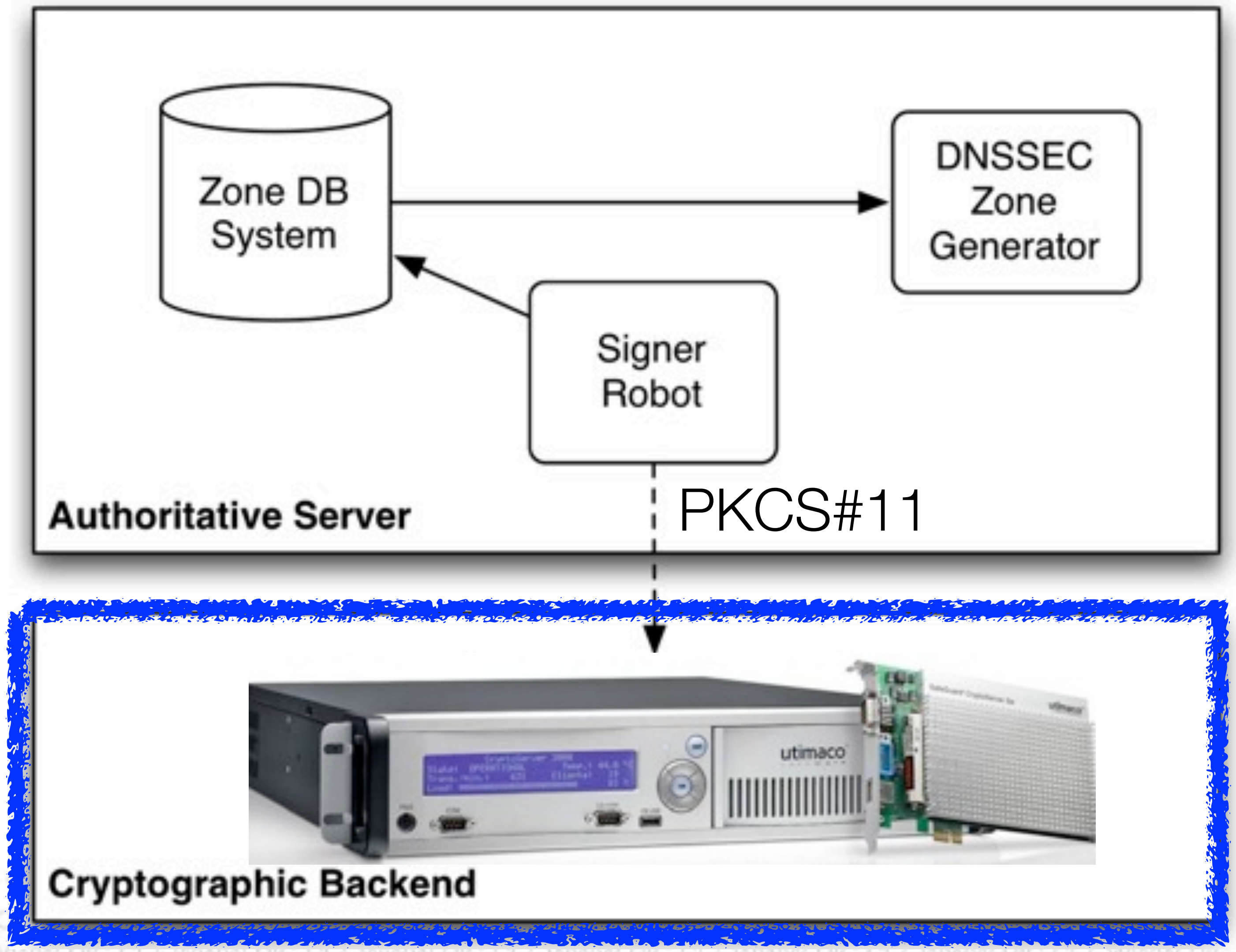


Zones need to be re-signed periodically.

Keys cannot be cloned(*)

- Server replication requires different keys
- Parent zone must know *keys* of its delegated zones (DS) in order to hold the chain of trust

DNSSEC Implementations

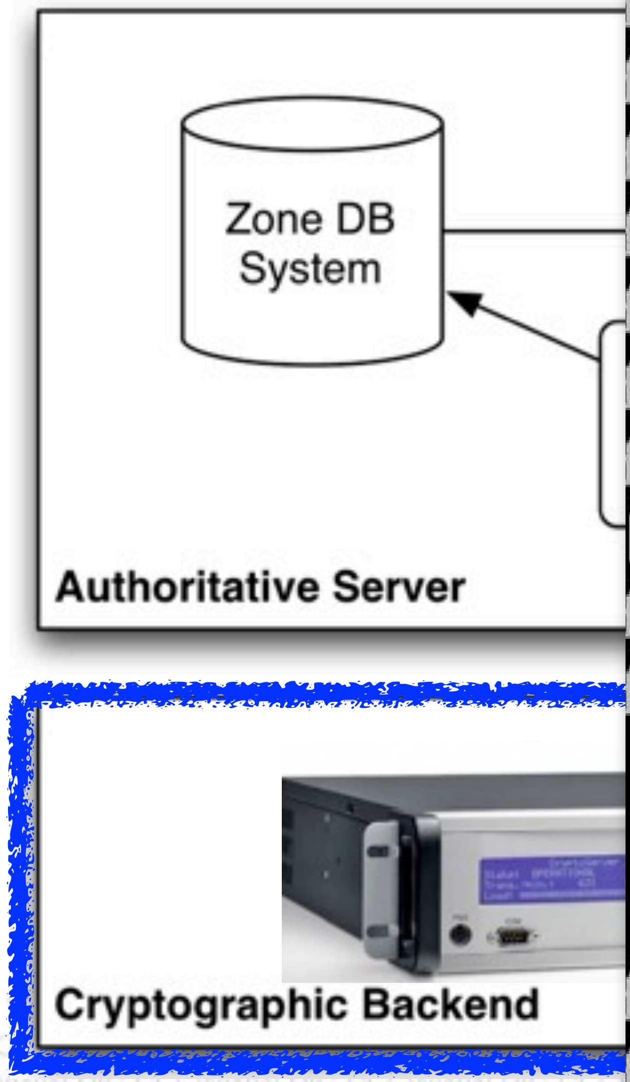


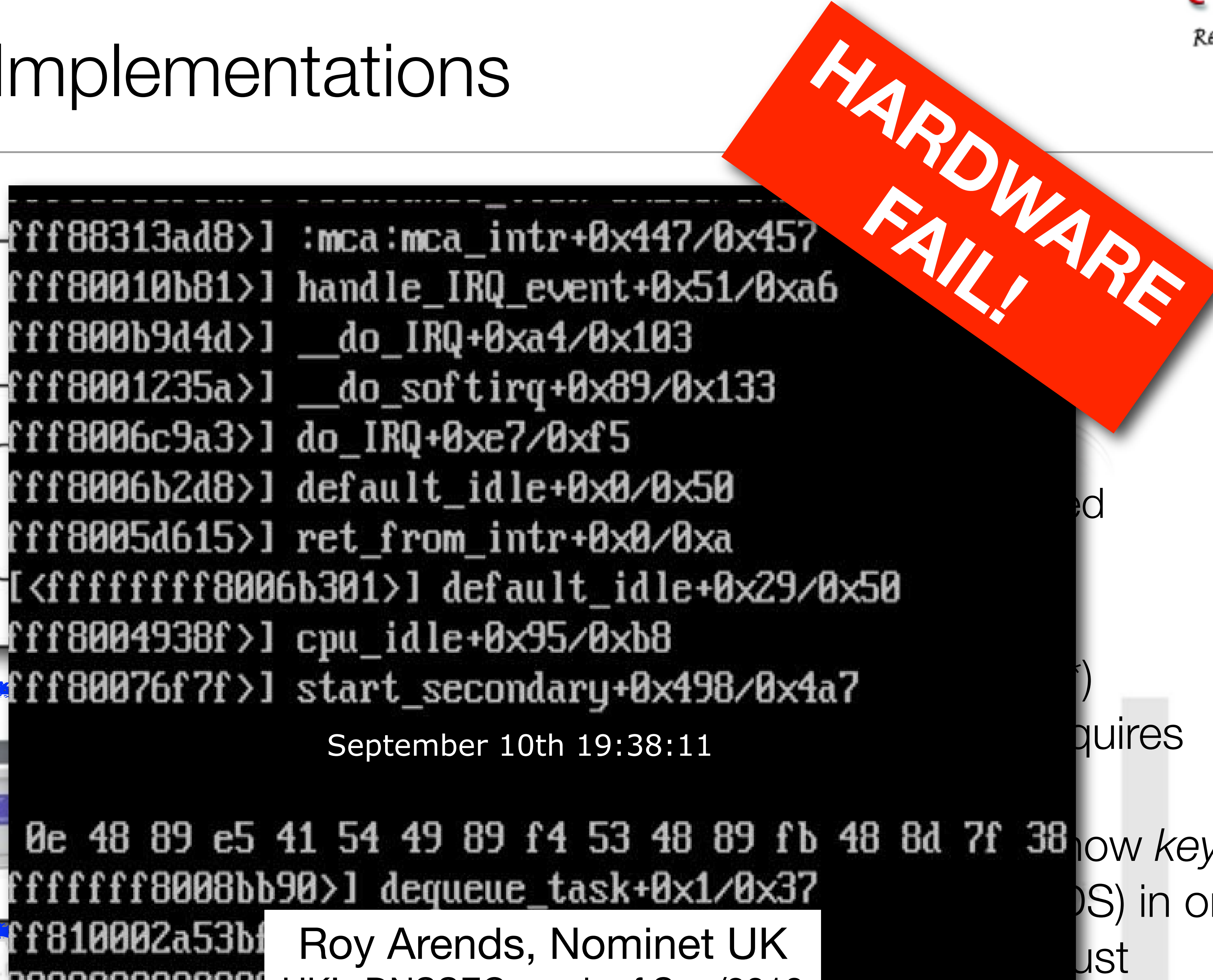
Zones need to be re-signed periodically.

Keys cannot be cloned(*)

- Server replication requires different keys
- Parent zone must know *keys* of its delegated zones (DS) in order to hold the chain of trust

DNSSEC Implementations





Roy Arends, Nominet UK
UK's DNSSEC crash of Sep/2010

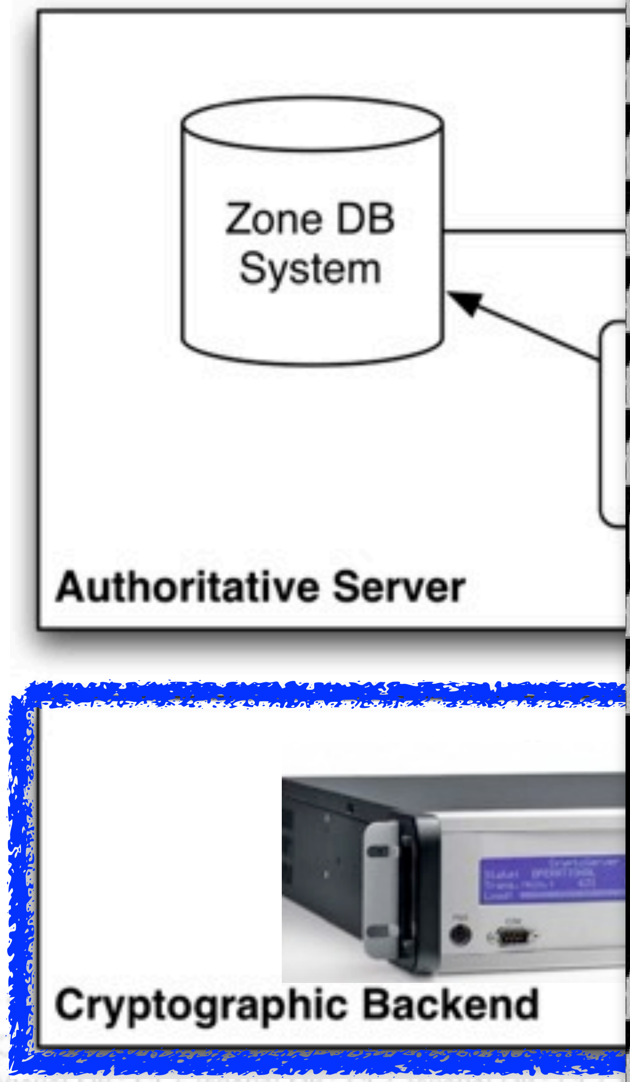
...ed

...)
...quires

...ow *keys* of
...S) in order
...ust

DNSSEC Implementations

HARDWARE FAIL!



Roy Arends, Nominet UK
UK's DNSSEC crash of Sep/2010

ed

)

quires

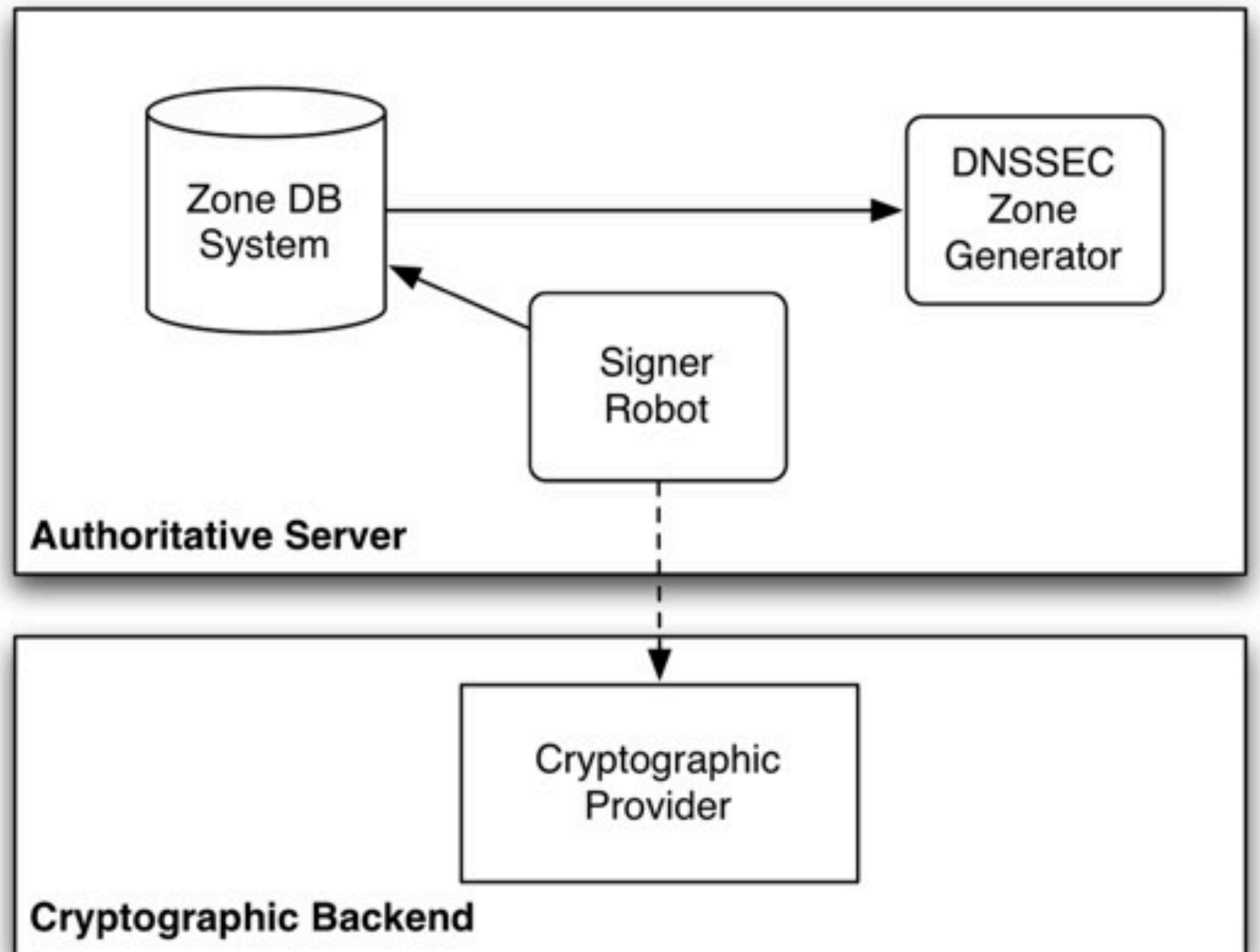
ow *keys* of

S) in order

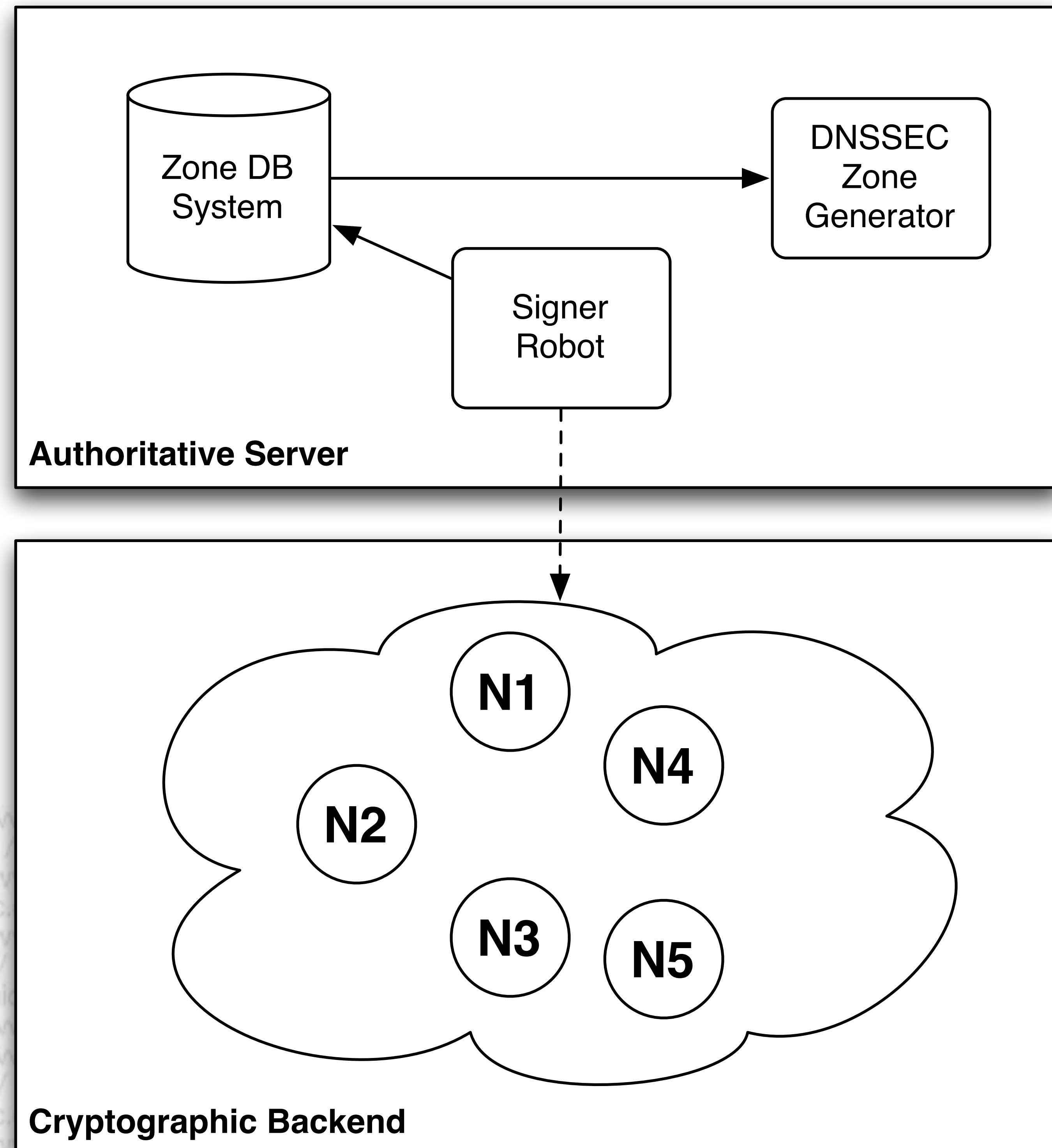
ust

Our work provides an alternative to HSM

Our Approach:
Distributed Cryptographic Backend



Our Approach: Distributed Cryptographic Backend



Our Approach: Distributed Cryptographic Backend

Our Approach:
Distributed Cryptographic Backend

- Distributed
  - Backend is implemented by means of **n** nodes
  - Private key is split into shares and distributed among these **n** nodes

Our Approach: Distributed Cryptographic Backend

- Distributed
  - Backend is implemented by means of **n** nodes
  - Private key is split into shares and distributed among these **n** nodes
- Fault-Tolerant
  - A subset of nodes can fail without system disruption

Our Approach:
Distributed Cryptographic Backend

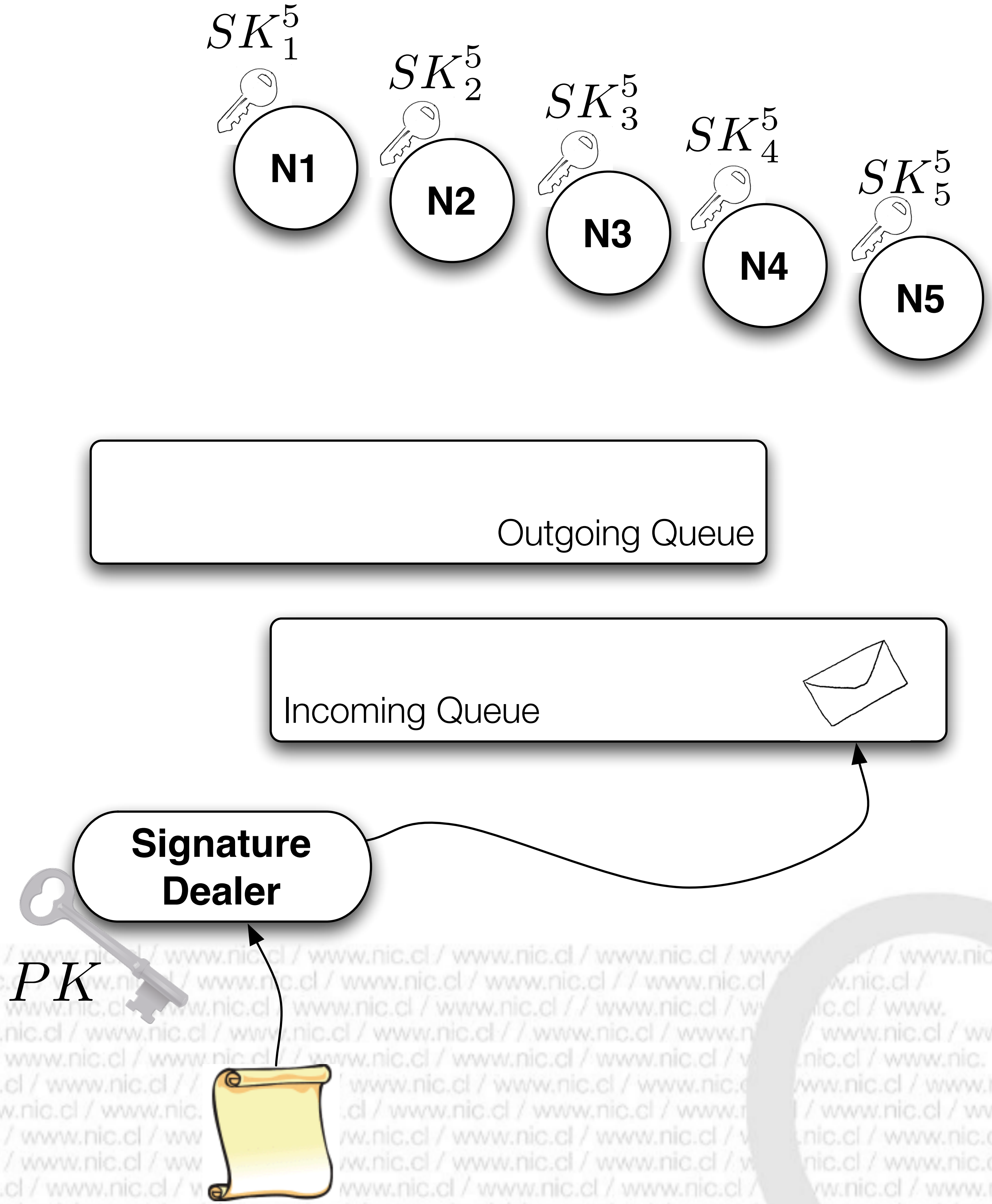
- Distributed
  - Backend is implemented by means of **n** nodes
  - Private key is split into shares and distributed among these **n** nodes
- Fault-Tolerant
  - A subset of nodes can fail without system disruption
- Robust
  - Failures and attacks are mitigated by implementing nodes in different programming languages and operating systems

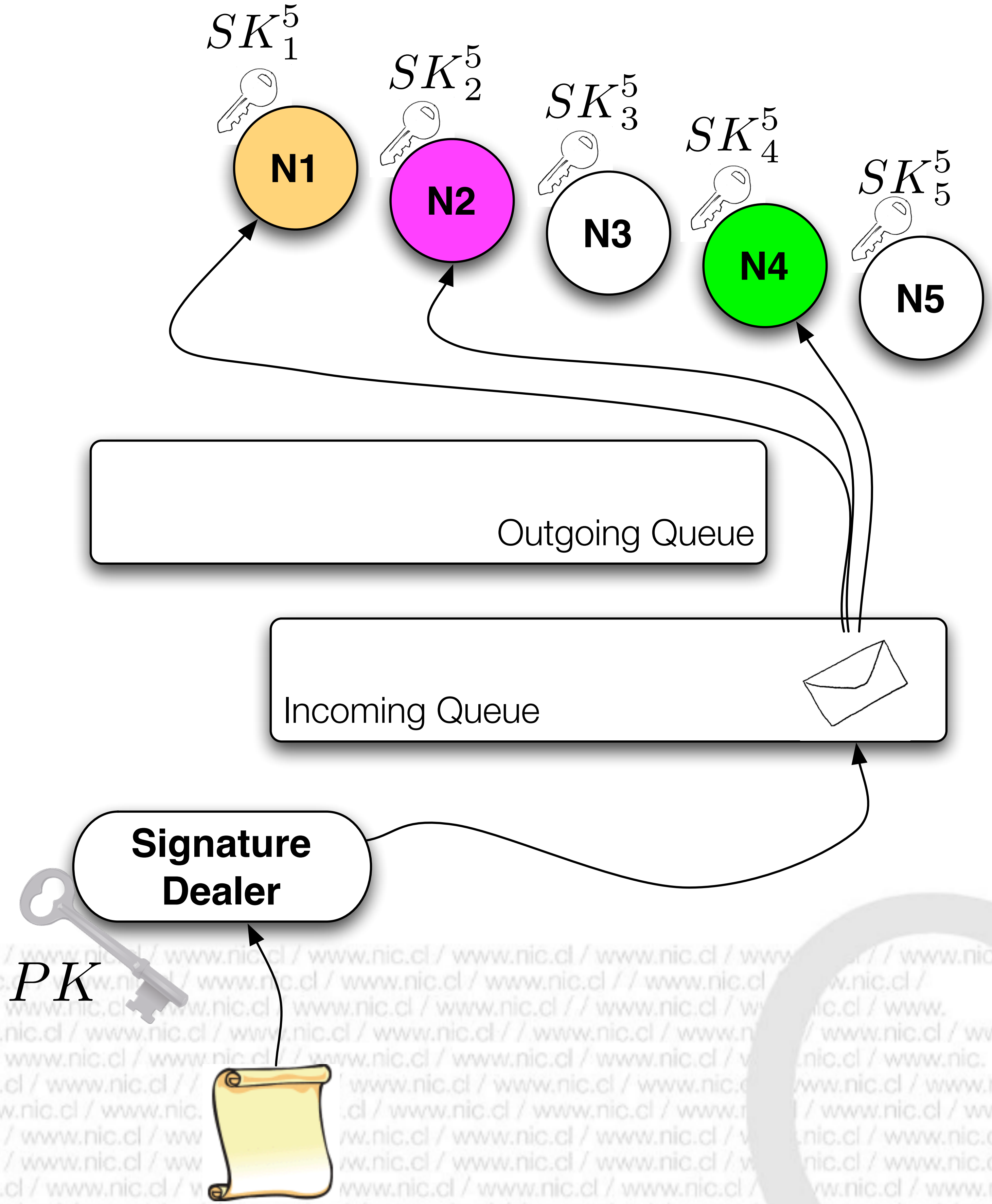
Our Approach:
Distributed Cryptographic Backend

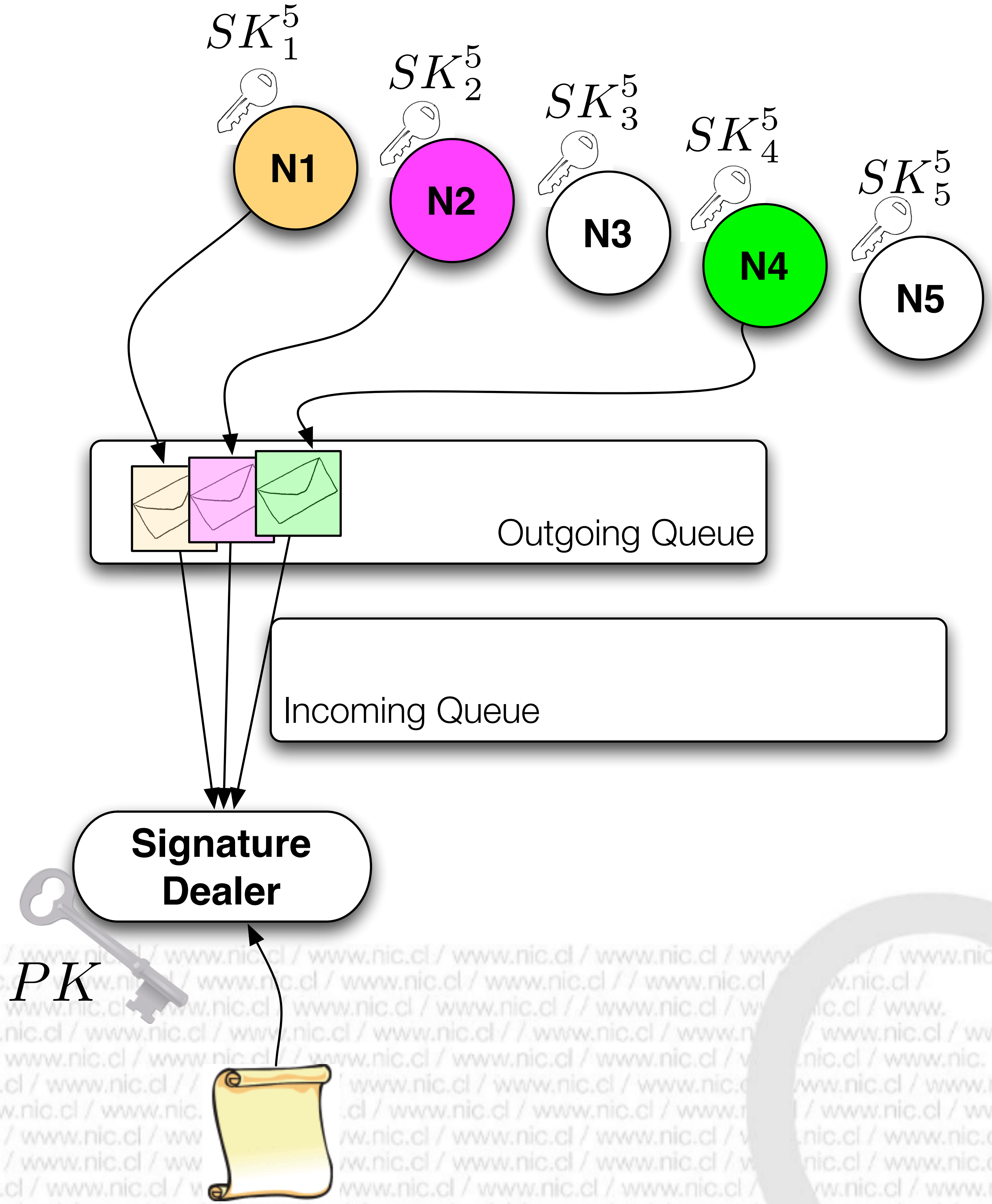
- Distributed
  - Backend is implemented by means of **n** nodes
  - Private key is split into shares and distributed among these **n** nodes
- Fault-Tolerant
  - A subset of nodes can fail without system disruption
- Robust
  - Failures and attacks are mitigated by implementing nodes in different programming languages and operating systems
- Secure
  - No one holds the complete private key
  - More than **k** the nodes must be compromised to authorize faked signatures

How does it work?

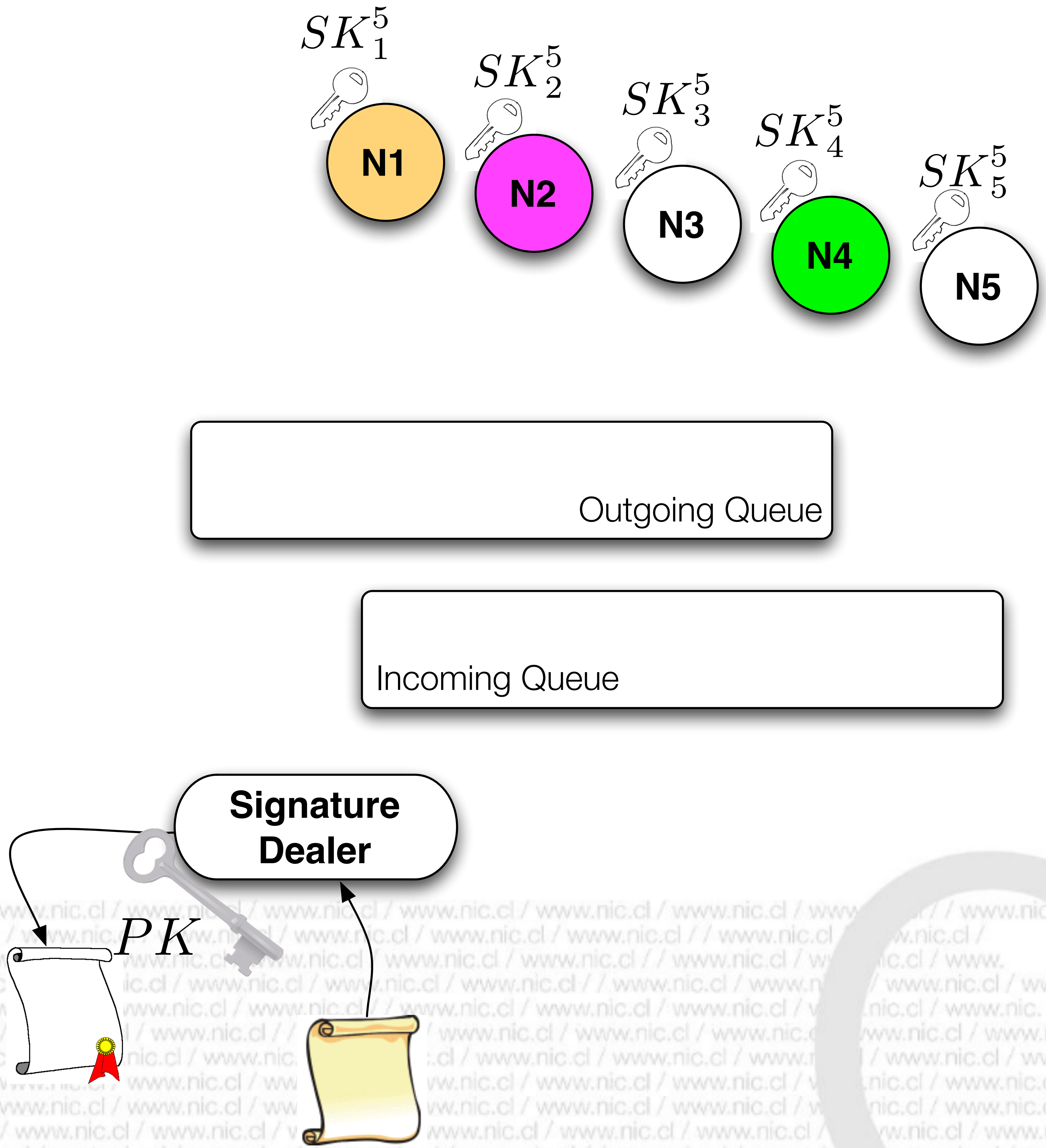
- Based on "*Practical threshold signatures*", by Victor Shoup in Eurocrypt 2000
- RSA Threshold Signature system **(n,k)**
  - Private Key SK is divided among **n** peers $\{SK\}_i^n$
  - Just **k** peers, **k<n**, are needed to create a signature
  - **k** shares are put together and validated against the Public Key PK
- Designed for systems with high volume of signatures (like DNSSEC)


SK_1^5
SK_2^5
SK_3^5
SK_4^5
SK_5^5
N1
N2
N3
N4
N5
Outgoing Queue
Incoming Queue
Signature Dealer
PK


SK_1^5
SK_2^5
SK_3^5
SK_4^5
SK_5^5
N1
N2
N3
N4
N5
Outgoing Queue
Incoming Queue
Signature Dealer
PK



SK_1^5
SK_2^5
SK_3^5
SK_4^5
SK_5^5
N1
N2
N3
N4
N5
Outgoing Queue
Incoming Queue
Signature Dealer
PK


SK_1^5
SK_2^5
SK_3^5
SK_4^5
SK_5^5
N1
N2
N3
N4
N5
Outgoing Queue
Incoming Queue
Signature Dealer
PK

Work in Progress

- Prototyped, but no benchmarks yet

Challenge	*Solution*	*Benefit*
Bottleneck at the Dealer Single point of failure	**P2P Architecture** Every node is a Dealer	Load balancing No single point of failure
Private key is created and then divided and distributed	**Distributed RSA** Key creation is distributed	Shares are directly created at the target nodes

Summary of the Approach

- Distributed cryptographic backend for DNSSEC
- Can replace HSMs, or complement them
- May be integrated with other DNSSEC engines (OpenDNSSEC, ...)

Advantages

- Distributed
- Robust
- Low-cost
- No one holds the complete key
- Risks can be bounded arbitrarily

Disadvantages

- Authentication with Dealer
- Number of shares is fixed upon key creation
- Slower than RSA
- Some bandwidth is used

Questions?

Thanks for your attention

More info: http://dnssec.niclabs.cl/

Threshold RSA

- Based on “*Practical threshold signatures*”, by Victor Shoup in Eurocrypt 2000

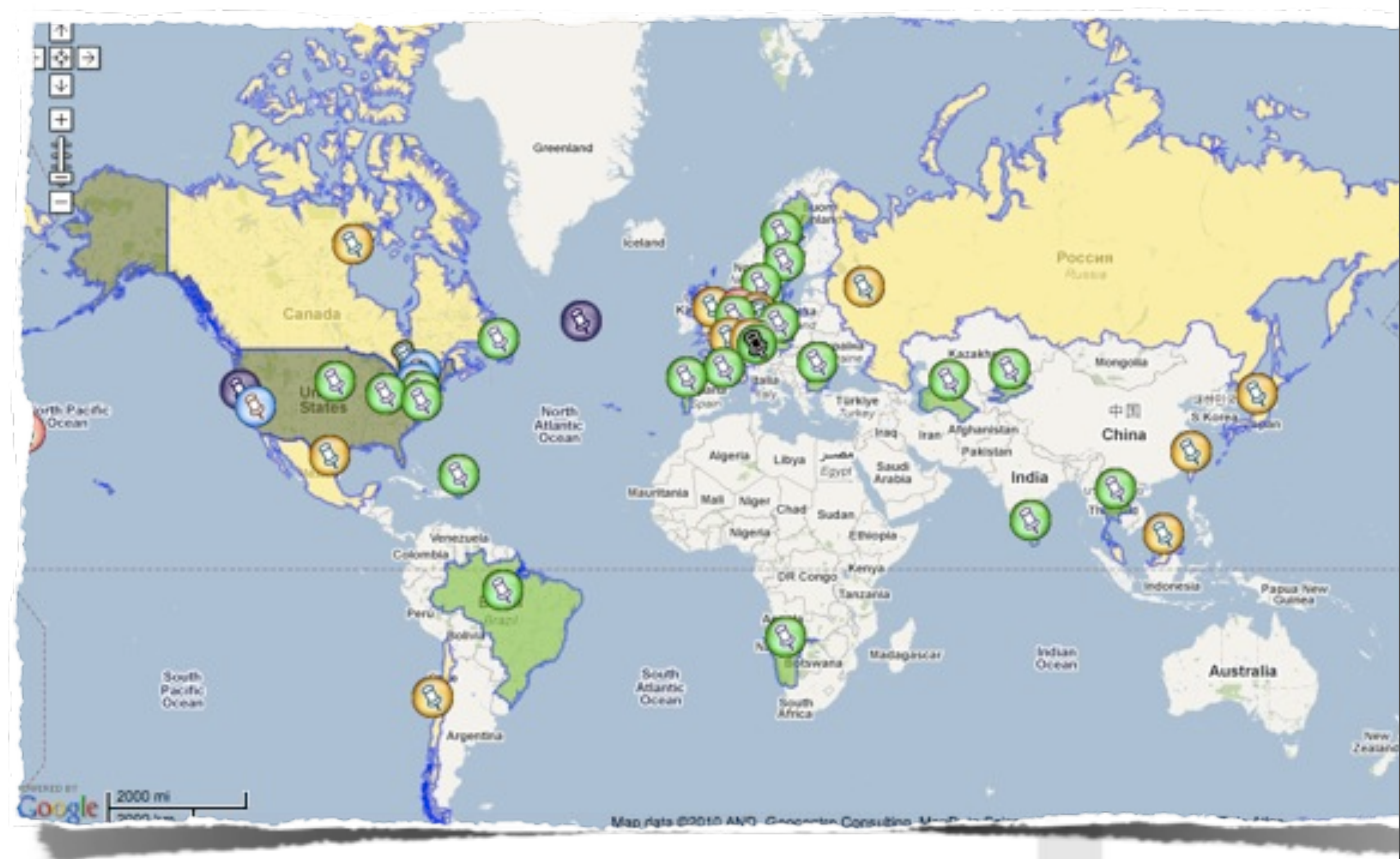
$$RSA = (PK, SK)$$

$$TC_{RSA} = (PK, \{SK\}_i^n, \{VK\}_i^n)$$

$$PK = (n, e) \quad n = pq$$

DNSSEC

- DNS SECurity extension to guarantee the origin and the authenticity of DNS records by means of Public Key Infrastructure.



- World Milestone: 15/Jul/2010 Root zone was signed and available for use.

- Roadmap for DNSSEC in NIC Chile => Deploying DNSSEC on CL servers

http://dnssec.niclabs.cl/