Deploying DNSSEC

Part II DNSSEC Mechanisms and deployment

AfriNIC-15,

Yaounde, 21th November 2011

Alain Aina P.

aalain@afrinic.net

Public Key Crypto (in one slide)

- Key pair: a secret (or private) key and a public key
  Simplified:
  - If you know the public key, you can decrypt data encrypted with the secret key
    - Usually an encrypted hash value over a published piece of information; the owner is the only person who can construct the secret. Hence this a signature
  - If you know the secret key, you can decrypt data encrypted with the public key
    - Usually an encrypted key for symmetric cipher
- PGP uses both, DNSSEC only uses signatures

DNSSEC Mechanisms

- New Resource Records
- Setting Up a Secure Zone
- Delegating Signing Authority
- DNSSEC Deployment Rollovers

New Resource Records

RRs and RRSets

- Resource Record:
  - name TTL class type rdata

```
www.nlnetlabs.nl.    7200    IN  A   192.168.10.3
```

- RRset: RRs with same name, class and type:

```
www.nlnetlabs.nl.  7200   IN   A  192.168.10.3
                        A 10.0.0.3
                        A     172.25.215.2
```

- RRSets are signed, not the individual RRs

New Resource Records

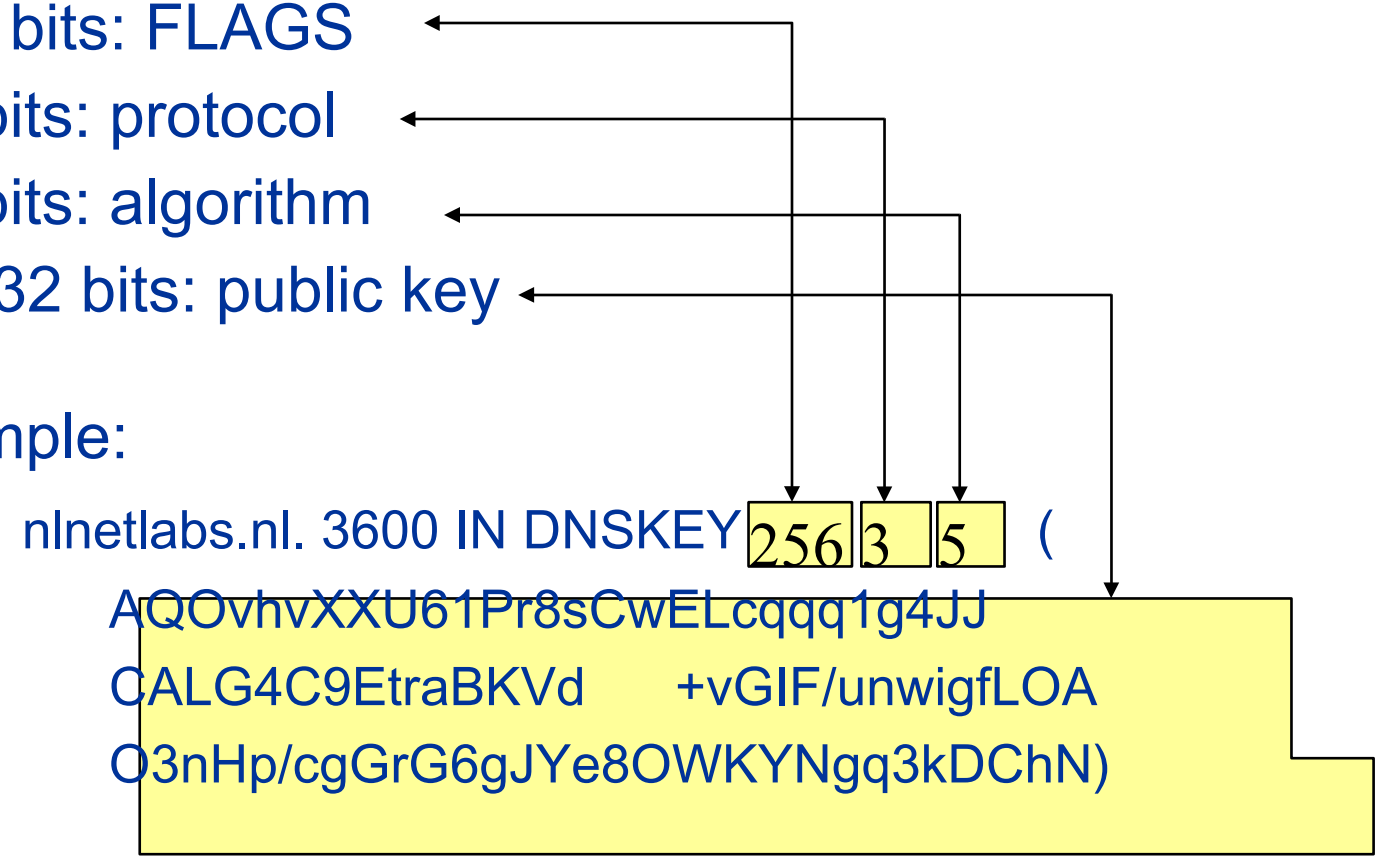
- Three Public key crypto related RRs
  - RRSIG Signature over RRset made using private key
  - DNSKEY Public key, needed for verifying a RRSIG
  - DS Delegation Signer; 'Pointer' for building chains of authentication

- One RR for internal consistency
  - NSEC Indicates which name is the next one in the zone and which typecodes are available for the current name
    - authenticated non-existence of data

DNSKEY RDATA

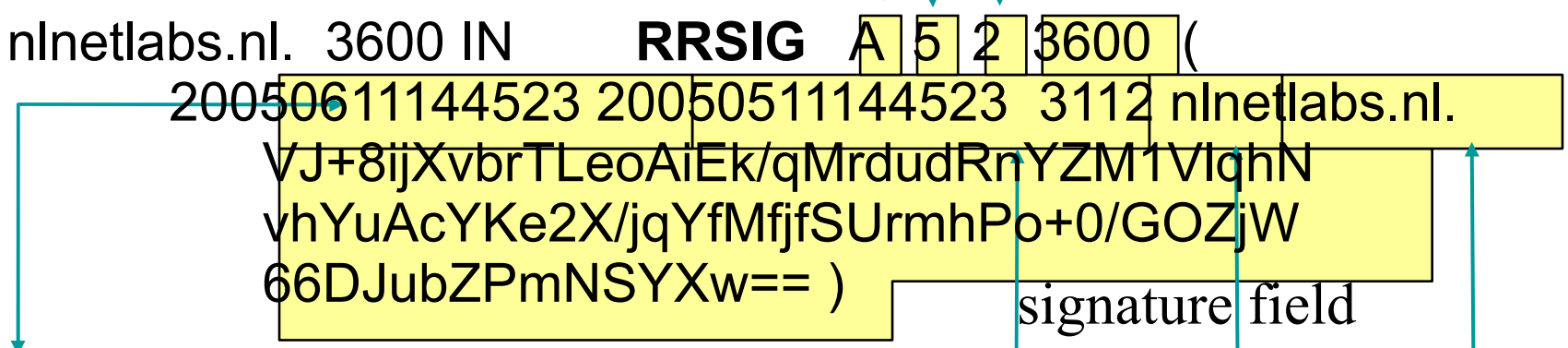
- 16 bits: FLAGS
- 8 bits: protocol
- 8 bits: algorithm
- N*32 bits: public key

Example:



RRSIG RDATA

- 16 bits - type covered
- 8 bits - algorithm
- 8 bits - nr. labels covered
- 32 bits - original TTL



- 32 bit - signature expiration
- 32 bit - signature inception
- 16 bit - key tag
- signer's name

Delegation Signer (DS)

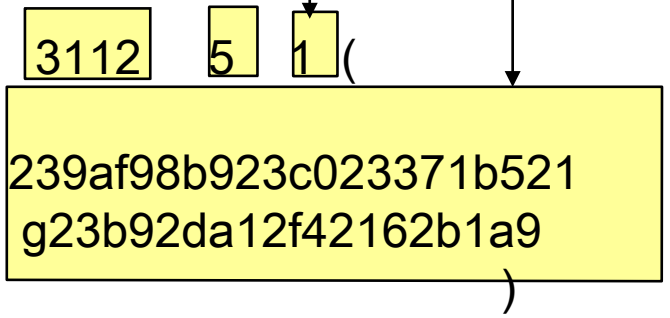
- Delegation Signer (DS) RR indicates that:
  - delegated zone is digitally signed
  - indicated key is used for the delegated zone

- Parent is authorative for the DS of the child's zone
  - Not for the NS record delegating the child's zone!
  - DS **should not** be in the child's zone

DS RDATA

- 16 bits: key tag
- 8 bits: algorithm
- 8 bits: digest type
- 20 bytes: SHA-1 Digest

```
$ORIGIN nlnetlabs.nl.
lab.nlnetlabs.nl.   3600 IN   NS  ns.lab.nlnetlabs.nl
lab.nlnetlabs.nl.   3600 IN   DS
```



NSEC RDATA

- Points to the next domain name in the zone
  - also lists what are all the existing RRs for "name"
  - NSEC record for last name "wraps around" to first name in zone
- N*32 bit type bit map
- Used for authenticated denial-of-existence of data
  - authenticated non-existence of TYPEs and labels

- Example:

```
www.nlnetlabs.nl. 3600 IN NSEC
```

nlnetlabs.nl.	A RRSIG NSEC

NSEC Records

- NSEC RR provides proof of non-existence
- If the servers response is Name Error (NXDOMAIN):
  - One or more NSEC RRs indicate that the name or a wildcard expansion does not exist
- If the servers response is NOERROR:
  - And empty answer section
  - The NSEC proves that the QTYPE did not exist
- More than one NSEC may be required in response
  - Wildcards
- NSEC records are generated by tools

NSEC Walk

- NSEC records allow for zone enumeration
- Providing privacy was not a requirement at the time
- Zone enumeration is a problem for some entities

- NSEC3
  - All RR names hashed
  - Hashed names are ordered
  - “opt-out” for unsecured delegations possibilities

Delegating Signing Authority

Chains of Trust

Using the DNS to Distribute Keys

- Secured islands make key distribution problematic
- Distributing keys through DNS:
  - Use one trusted key to establish authenticity of other keys
  - Building chains of trust from the root down
  - Parents need to sign the keys of their children
- Only the root key needed in ideal world
  - Parents always delegate security to child

Key Problem

- Interaction with parent administratively expensive
  - Should only be done when needed
  - Bigger keys are better
- Signing zones should be fast
  - Memory restrictions
  - Space and time concerns
  - Smaller keys with short lifetimes are better

Key Functions

- Large keys are more secure
  - Can be used longer ☺
  - Large signatures => large zonefiles ☹
  - Signing and verifying computationally expensive ☹
- Small keys are fast
  - Small signatures ☺
  - Signing and verifying less expensive ☺
  - Short lifetime ☹

Key solution: More Than One Key

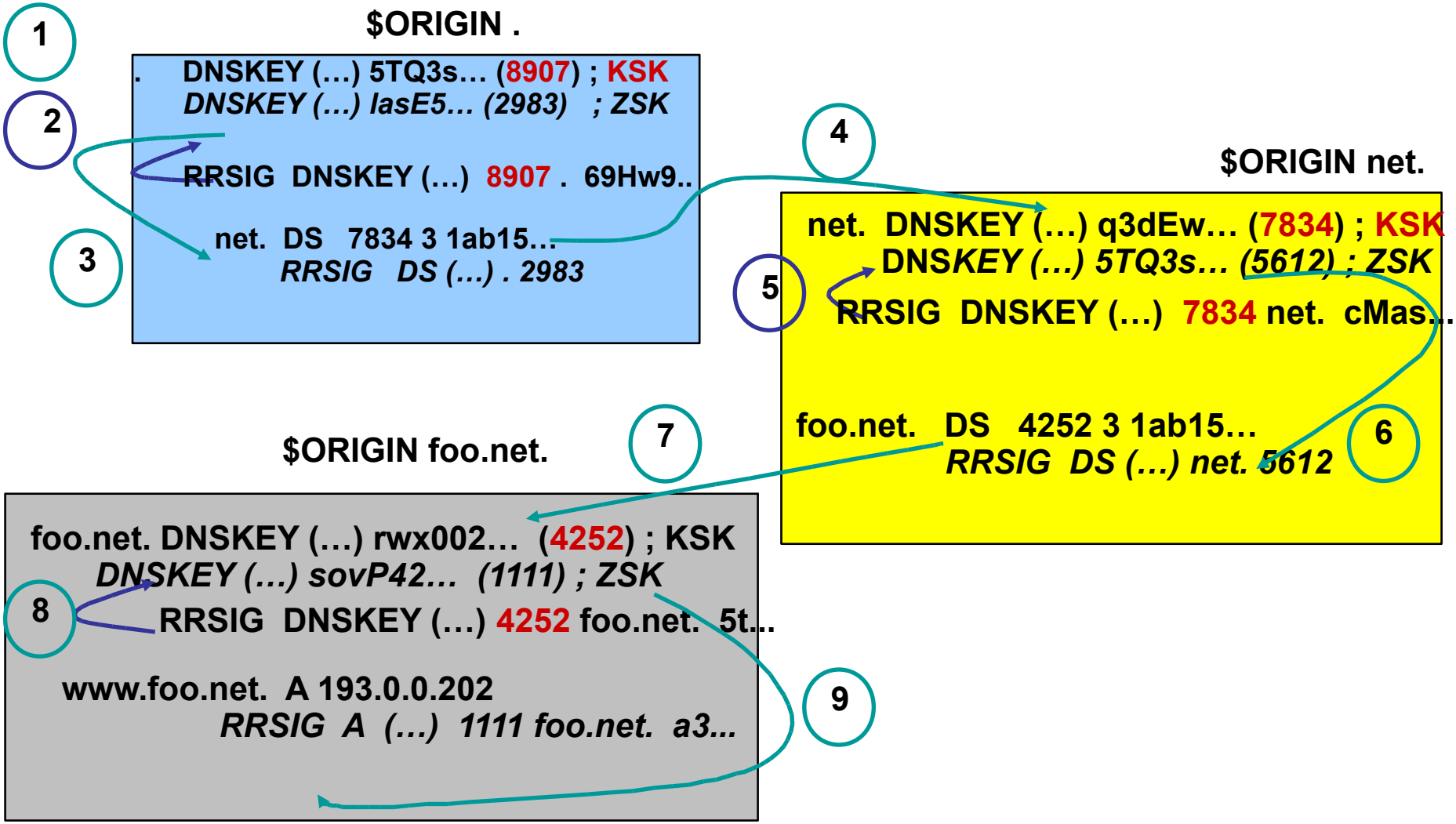
- RRsets are signed, not RRs
- DS points to specific key
  - Signature from that key over DNSKEY RRset transfers trust to all keys in DNSKEY RRset
- Key that DS points to only signs DNSKEY RRset
  - Key Signing Key (KSK)
- Other keys in DNSKEY RRset sign entire zone
  - Zone Signing Key (ZSK)

Initial Key Exchange

- Child needs to:
  - Send key signing keyset to parent
- Parent needs to:
  - Check child's zone
    - for DNSKEY & RRSIGs
  - Verify if key can be trusted
  - Generate DS RR

y configured
d key: . 8907

Walking the Chain of Trust



Security Status of Data (RFC4035)

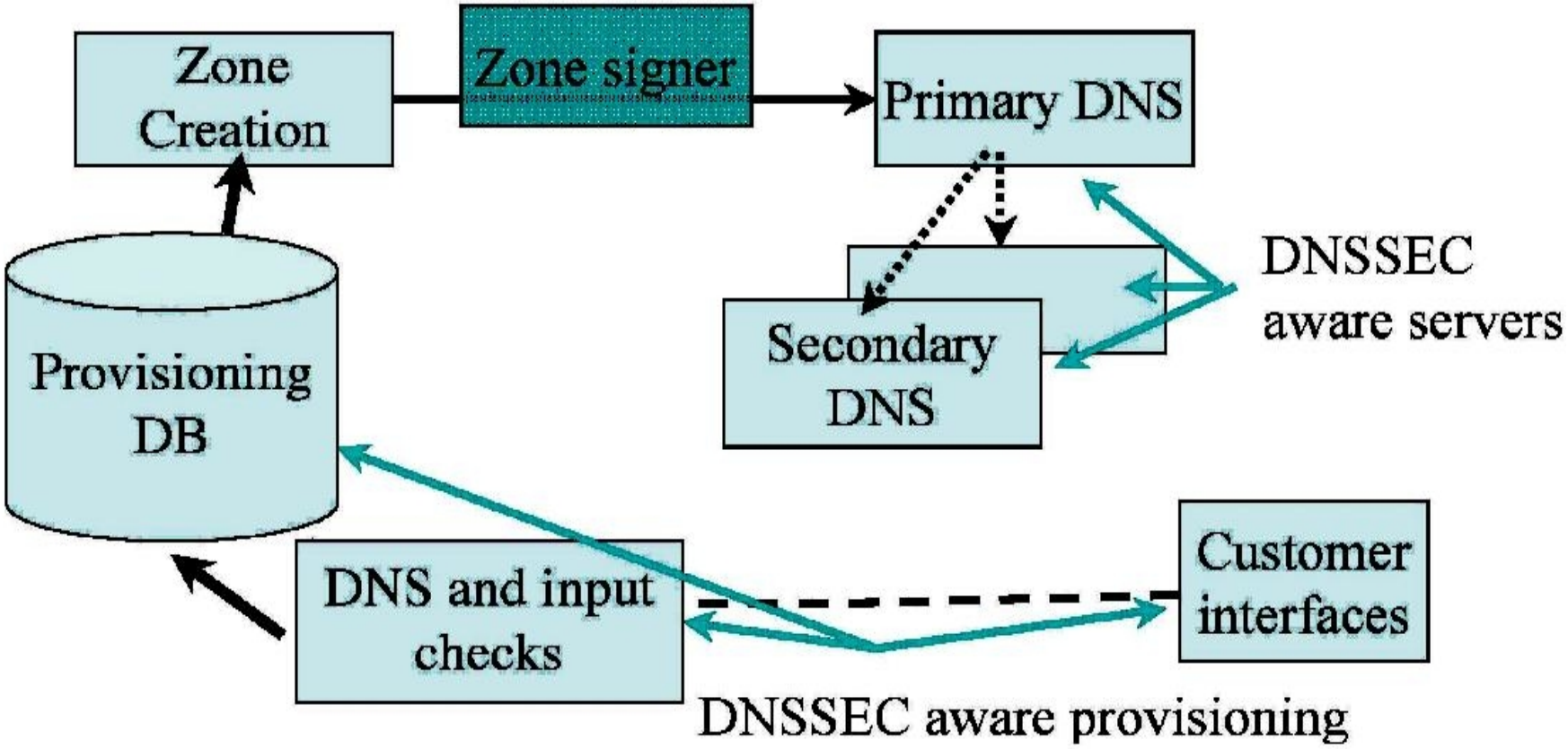
- Secure
  - Resolver is able to build a chain of signed DNSKEY and DS RRs from a trusted security anchor to the RRset
- Insecure
  - Resolver knows that it has no chain of signed DNSKEY and DS RRs from any trusted starting point to the RRset
- Bogus
  - Resolver believes that it ought to be able to establish a chain of trust but for which it is unable to do so
  - May indicate an attack but may also indicate a configuration error or some form of data corruption
- Indeterminate
  - Resolver is not able to determine whether the RRset should be signed

DNSSEC DEPLOYMENT

DNSSEC Deployment Tasks

- Key maintenance policies and tools
  - Private key use and protection
  - Public key distribution
- Zone signing and integration into the provisioning chain
- DNS server infrastructure
- Secure delegation registry changes
  - Interfacing with customers

DNSSEC Architecture modification



Key Maintenance

- DNSSEC is based on public key cryptography
  - Data is signed using a private key
  - It is validated using a public key

Operational problems:

- Dissemination of the public key
- Private key has a '*best before*' date
  - Keys change, and the change has to disseminate

DNSSEC Policy & Practice Statement

- draft-ietf-dnsop-dnssec-dps-framework

```
This document presents a framework to assist writers of DNSSEC Policy
  and Practice Statements such as Domain Managers and Zone Operators on
  both the top-level and secondary level, who is managing and operating
  a DNS zone with Security Extensions (DNSSEC) implemented.

  In particular, the framework provides a comprehensive list of topics
  that should be considered for inclusion into a DNSSEC Policy
  definition and Practice Statement.
```

- ICANN DPS for root zone
  - http://www.root-dnssec.org/wp-content/uploads/2010/06/icann-dps-00.txt

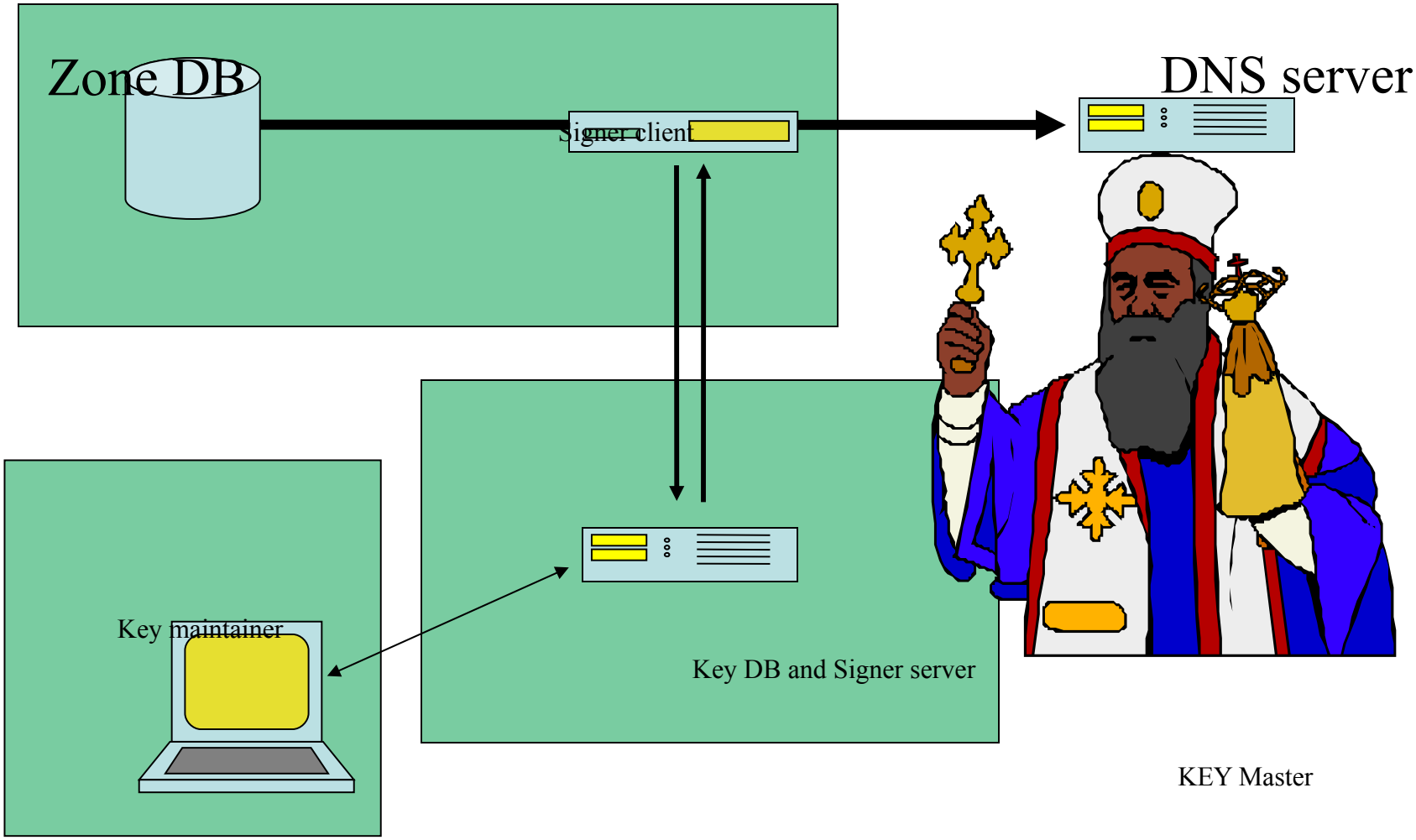
Public Key Dissemination

- In theory only one trust-anchor needed that of the root
  - How does the root key get to the end user?
  - How is it rolled?
- In absence of hierarchy, there will be many trust-anchors
  - How do these get to the end-users?
  - How are these rolled?
- These are open questions,making early deployment difficult.
- DLV registries(https://secure.isc.org/index.pl?/ops/dlv/)

Key Management

- There are many keys to maintain
  - Keys are used on a per zone basis
    - Key Signing Keys and Zone Signing Keys
  - During key rollovers there are multiple keys
    - In order to maintain consistency with cached DNS data
    - RFC4641
- Private keys need shielding

Private Key Maintenance Basic Architecture



Maintaining Keys and Signing Zones

- The KeyDB maintains the private keys
  - It ‘knows’ rollover scenarios
  - UI that can create, delete, roll keys without access to the key material
  - Physically secured
- The signer ties the Key DB to a zone
  - Inserts the appropriate DNSKEYs
  - Signs the the zone with appropriate keys
- Strong authentication

Infrastructure

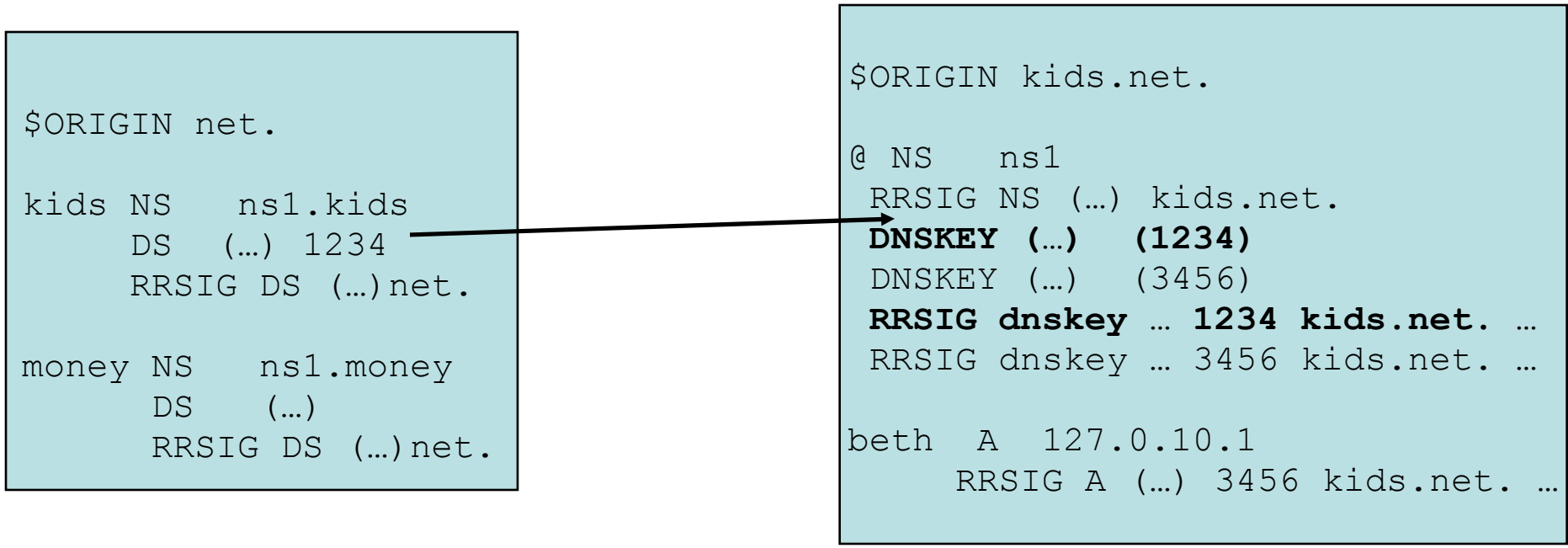
- One needs primary and secondary servers to be DNSSEC protocol aware
- We have concerns about Firewalls/IDS/IPS on DNS packet size and EDNS0
  - http://www.icann.org/committees/security/sac016.htm
- We had a number of concerns about memory, CPU, network load
  - Research done at RIPE-NCC and published as RIPE 352

Infrastructure

- Bandwidth increase is caused by many factors
  - Hard to predict but fraction of DO bits in the queries is an important factor
- CPU impact is small, Memory impact can be calculated
- Don’t add DNSKEY RR set in additional

Parent-Child Key Exchange

- In the DNS the parent signs the "Delegations Signer" RR
  - A pointer to the next key in the chain of trust



- DNSKEY or DS RR needs to be exchanged between parent and child

Underlying Ideas

- The DS exchange is the same process as the NS exchange
  - Same authentication/authorization model
  - Same vulnerabilities
  - More sensitive to mistakes
- Integrate the key exchange into existing interfaces
  - Customers are used to these
- Include checks on configuration errors
  - DNSSEC is picky
- Provide tools
  - To prevent errors and guide customers

Questions ???