# DNSSEC Key management

## João Damas
## ISC

# Contents

- DNS and keys
- DNSSEC keys
- Elements of DNSSEC
- The chain of trust
- Rollover
- Key storage
- Managing it all

# DNS and keys

- TSIG
  - shared secret
- DNSSEC
  - Public key cryptography

# DNSSEC keys

- Public key crypto keys as used in many other places
- A few bytes to identify protocols in use
  - also used to signal other features of DNSSEC

# Elements of DNSSEC

- Keys
- Signatures
- Delegation signers

# Keys

- Operational convenience
  - Key signing key
  - Zone signing key
- Signalling
  - NSEC vs NSEC3

# Key Signing Key

- The key that signs other keys
  - the SEP bit

```
isc.org.     IN     DNSKEY  257 3 5 BEAAAAOhHQDB.....

isc.org.     IN     DNSKEY  256 3 5 BEAAAAO6L6Ba.....
```

# Zone signing key

- The one that signs the zone

```
isc.org.     IN     DNSKEY  257 3 5 BEAAAAOhHQDB.....

isc.org.     IN     DNSKEY  256 3 5 BEAAAAO6L6Ba.....
```

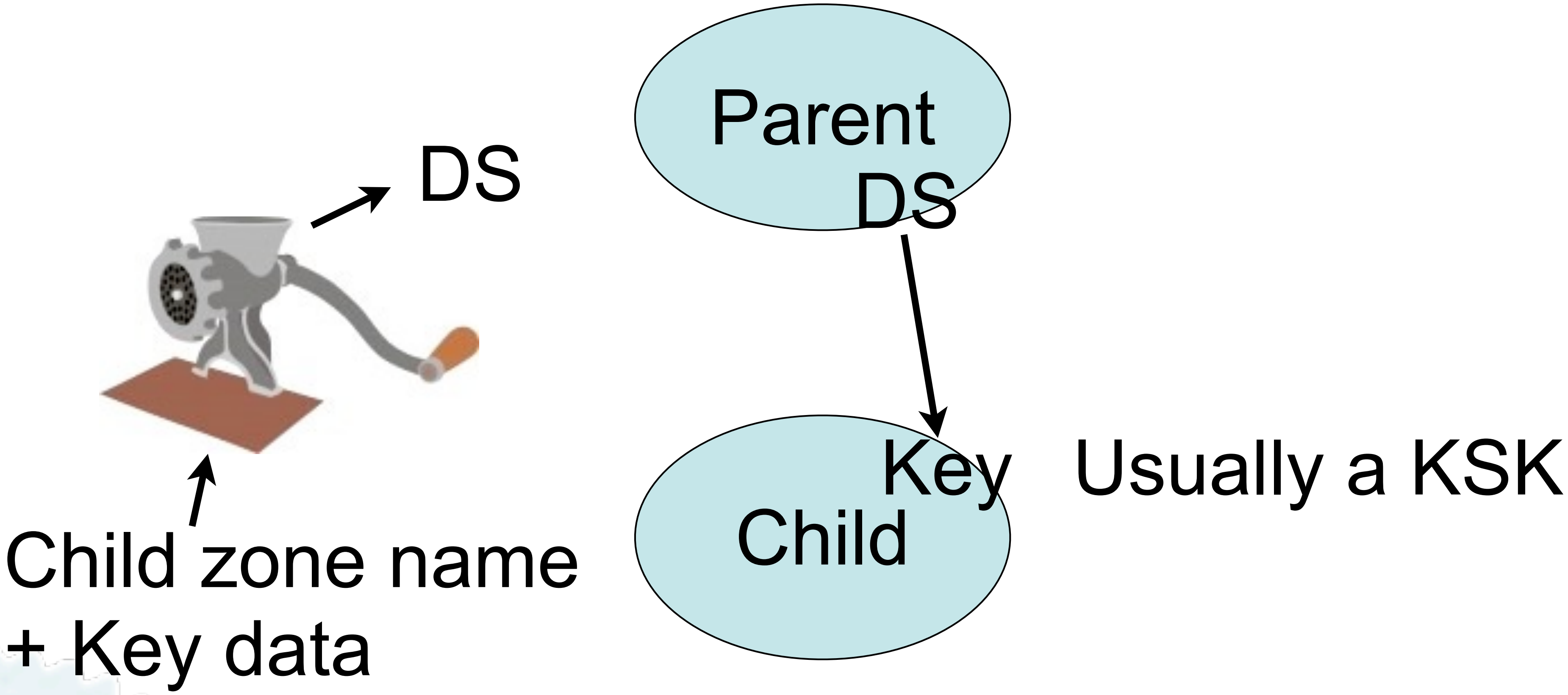
# Signatures

- Common practice is to use the KSK to sign the set of keys in the zone...
- ... and to use the ZSK to sign all other content of the zone
- Signatures are what proves the data is unaltered when it reaches the DNS client

# Delegation signers

- How to link all the zones to secure the DNS tree?
- DS records
  - –a hash of the zone name and the key data
  - –a few fields to identify protocols in use
- Goes into the parent zone

# The chain of trust



DS

Parent

DS

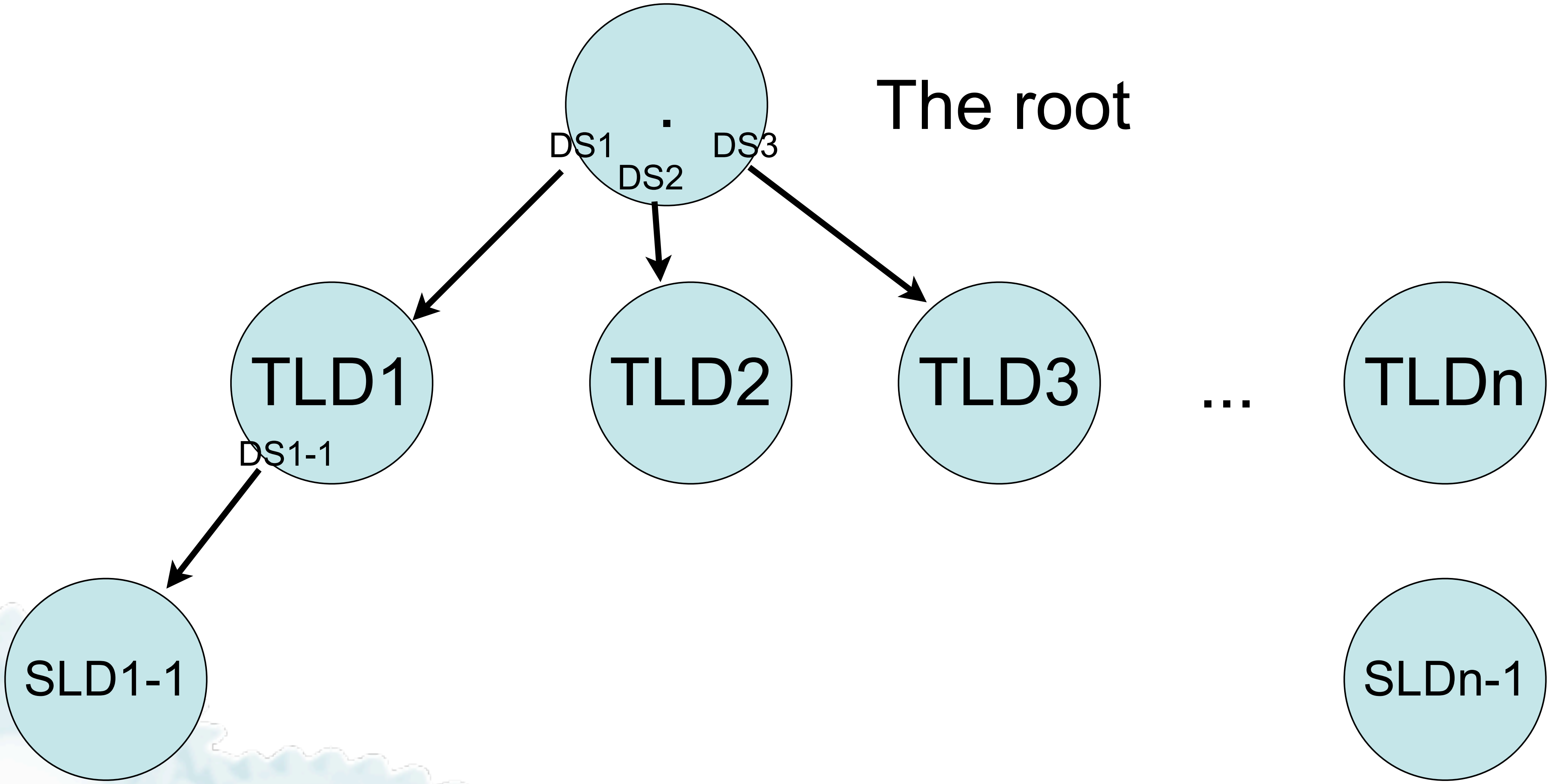
Key

Usually a KSK

Child

Child zone name
+ Key data

# The chain of trust



# Why rollover?

- Keys have no expiration dates
  - –yet time leaves traces in all of us
- Algorithms broken
  - –rollover key and algorithms in use
- Unauthorised access to private key

# Key rollover

- ZSK rollover
  - Does **not** require communication with parent zone
- KSK rollover
  - **requires** a new DS record at the parent zone

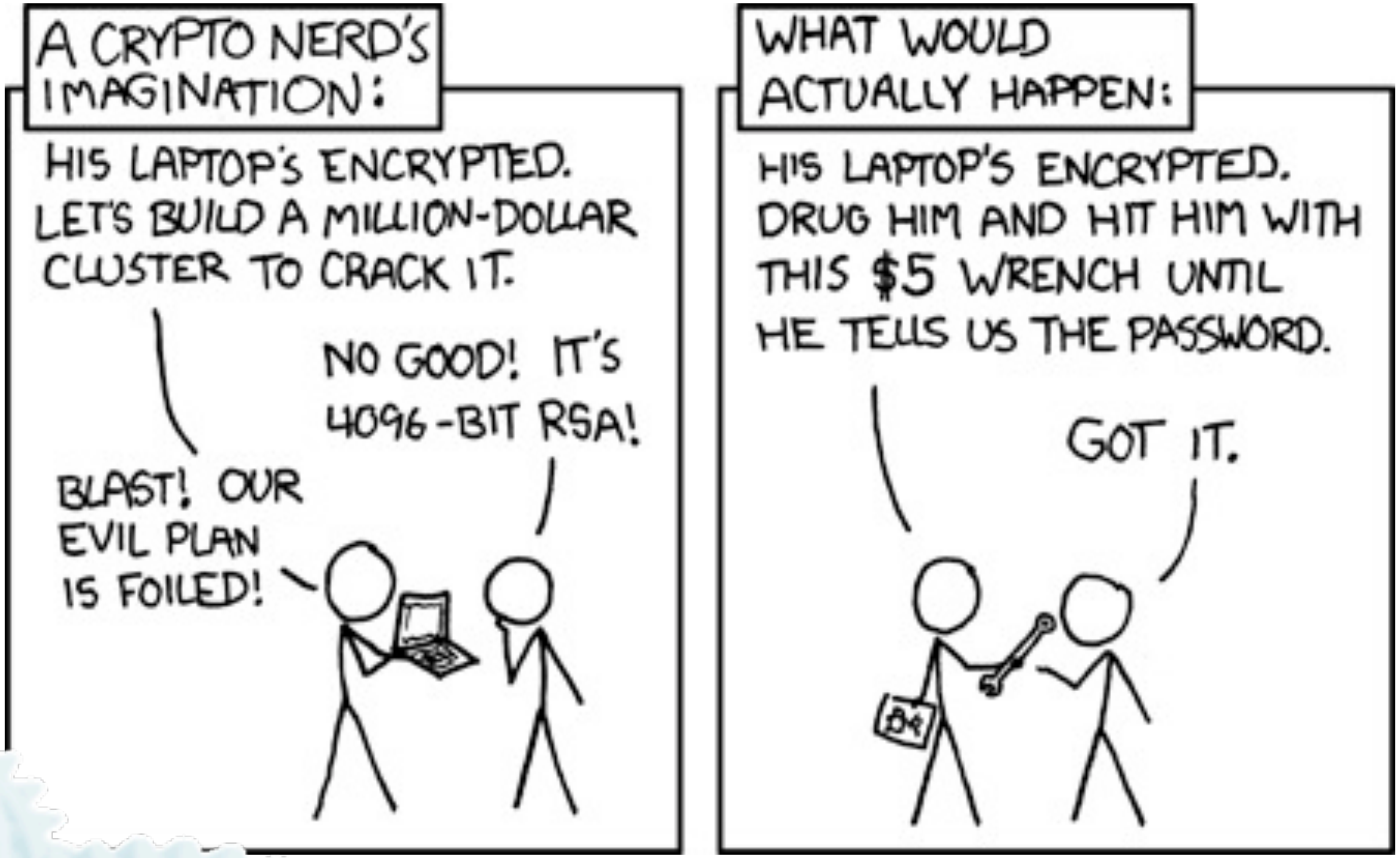
# How to rollover?

- Pre-publication
  - beware the extra data
- Double signing
  - beware the TTLs

# Key storage

- Basic question
  - Which is more important, the key or the zone data?

# Key storage


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

***http://xkcd.com/538/***

# Key storage

- File system
- dedicated, offline machine
- HSM

# How to manage all of this

- Decide what you want/need (policy)
- Use software to automate
  - BIND 9.7+
  - ZKT
  - OpenDNSSEC

# Thanks

- Alan Clegg of ISC

# Questions?

# joao@isc.org