nominet

# Key and Signing Policy

John Dickinson

Introduction

# Key and Signing Policy

## Why do we need KASP

- We have new tools to generate keys and use them to sign
  - How will we use them?
- We will need continuous signing for co.uk
  - How will it work?
  - What parameters will BIND need to know?

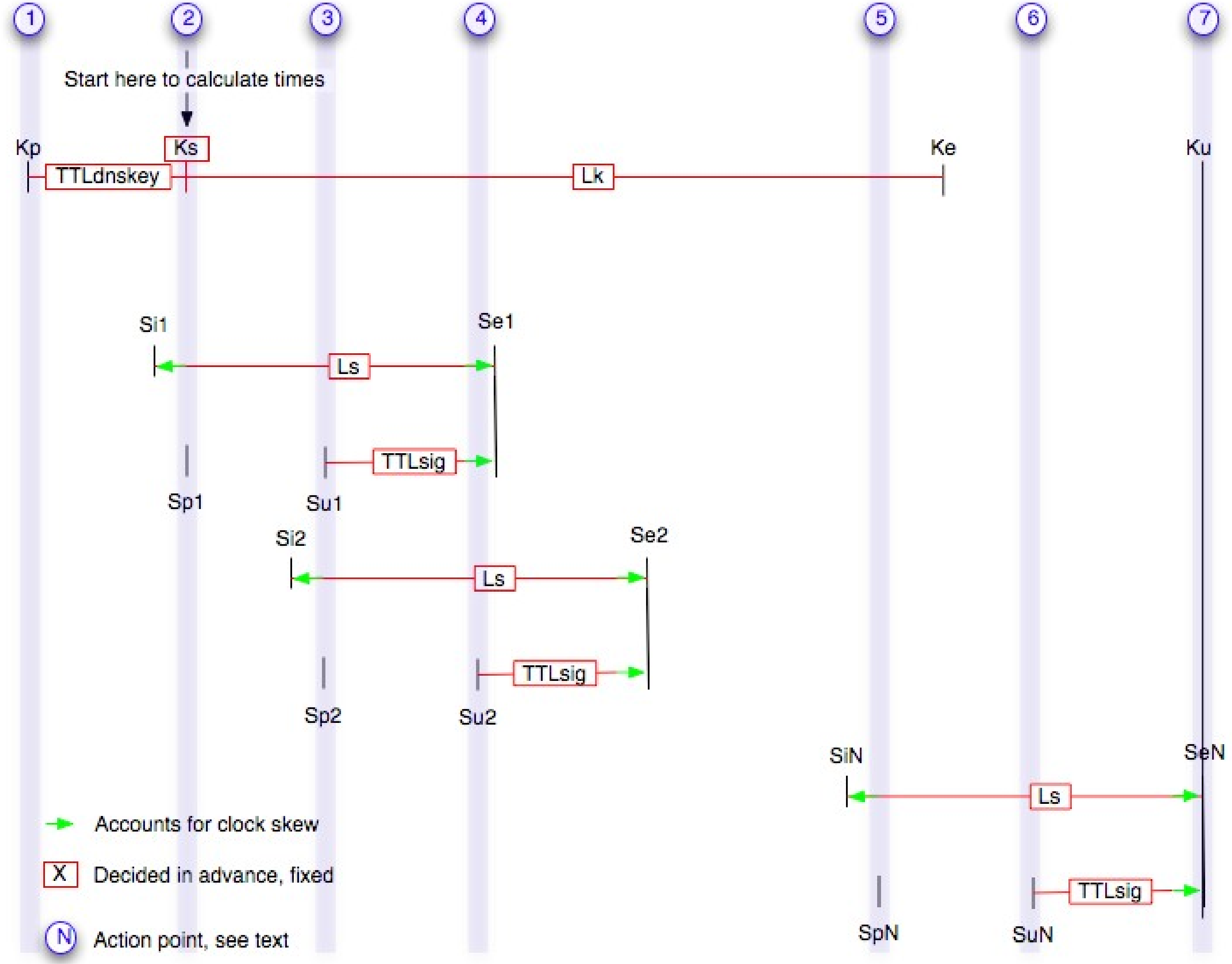
# Key and Signing Policy

## Why do we need KASP

- We thought about the timelines involved in signing
- We started to think about how we would use these tools
- We trained our operational teams with the existing tools
  - What did they think?
  - What was hard?

# Authoritative Servers

## KASP Timelines



# KASP

## Key Generation Example

```
dnssec-keygen -a rsasha1 -b 512 -n zone example.com
Kexample.com.+005+63933

dnssec-keygen -a rsasha1 -b 2048 -f KSK -n zone example.com
Kexample.com.+005+57514
```

- Could we do this if the keys are in an HSM?
  - Why do the keys care about
    - The zone?
    - If they will be used as KSK’s or ZSK’s?
- So, our key generator will be very different
  - How will we know what zone and use the key will have?

Authoritative Servers

# KASP

## Signing Example

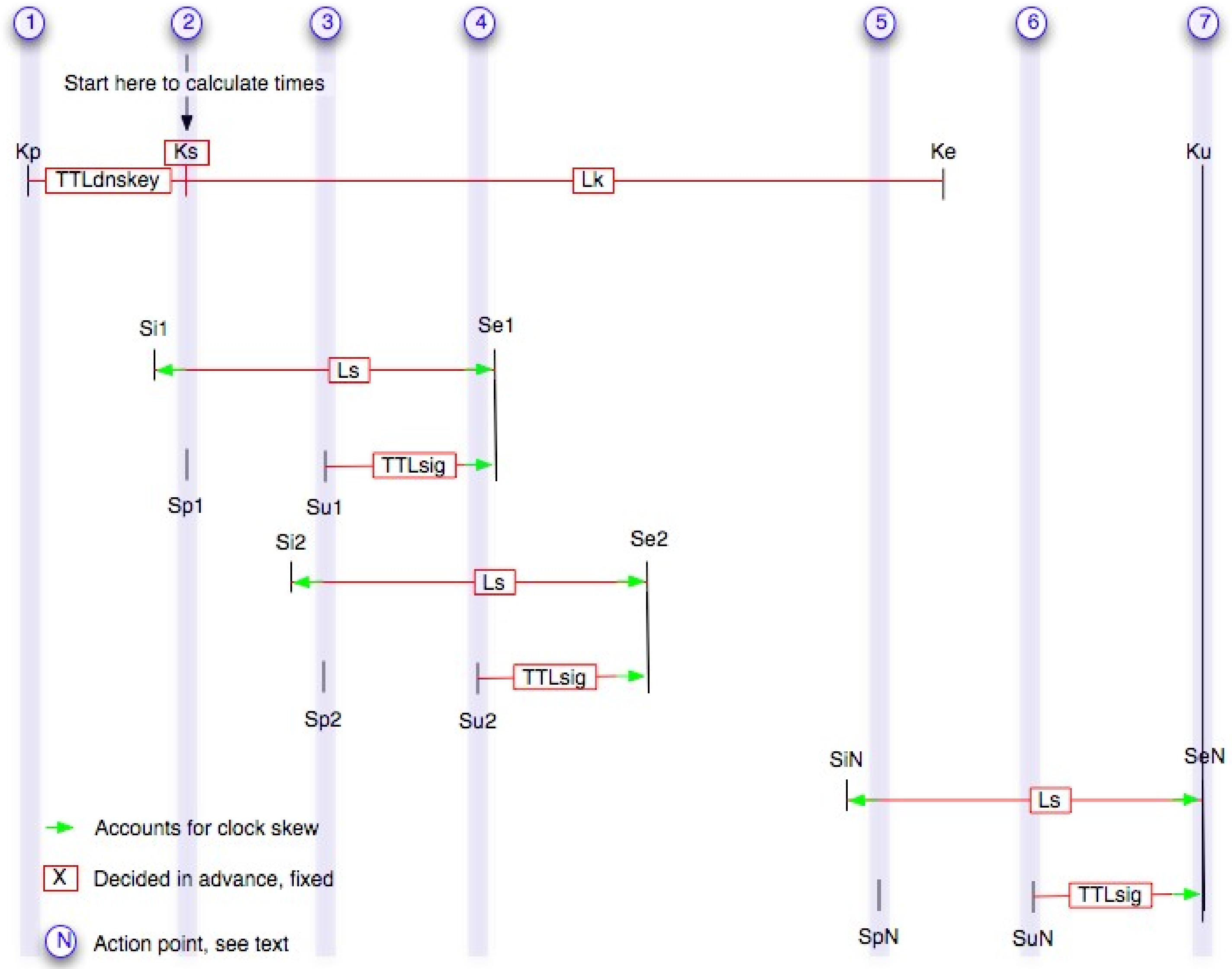
```
cat Kexample.com.+005+57514.key >> example.com
cat Kexample.com.+005+63933.key >> example.com

dnssec-signzone -o example.com -t -k Kexample.com.+005+57514
example.com Kexample.com.+005+63933
```

- Why do I need to use cat?
- How do I know which key goes with the -k option?
- What happens if I get it wrong?
- What’s the -o option again?
- Can I use one key with many zones?

## Authoritative Servers

# KASP Timelines



# KASP

## What is KASP?

- A “database” that stores information about zones, keys and signing policy
- An API to access the database
- To be used by tools and name servers to decide
  - When to sign and re-sign
  - What zones to sign
  - Which keys to use
  - Where to find the keys
  - When to publish and withdraw keys from the zone.

Authoritative Servers

# KASP

## What is KASP?

- Intended to work with both HSM based keys and keys on disk.
- For example
  - Why are on-disk keys in files called `Kexample.com.+005+57514.*`
  - How will that help us use the keys?

# KASP

## Where are we now?

- We are writing
  - An API
  - XML schema
  - Converting our key generator and signer to use KASP
- We will publish this soon.
- Please tell us what you think.
- See http://blog.nominet.org.uk/tech for more info.