DNS and DNSSEC Management and Monitoring Changes Required During A Transition To DNSSEC

Wes Hardaker
<wes.hardaker@parsons.com>

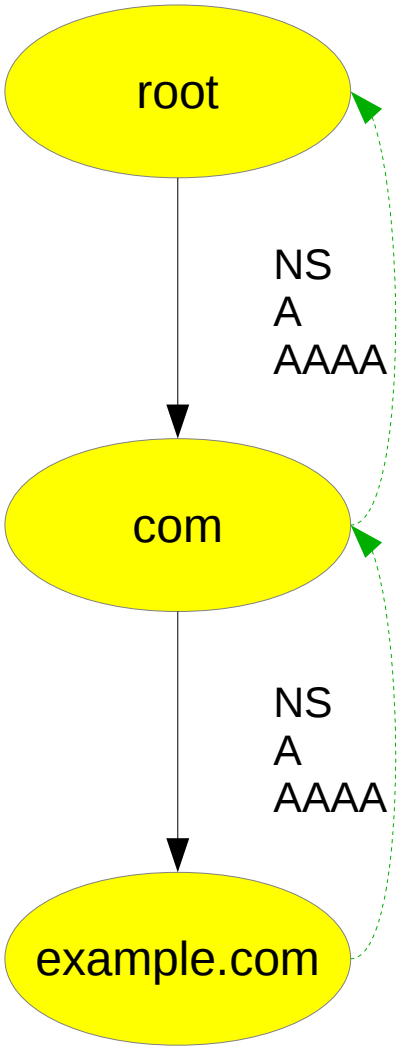
Overview

- Business Model Changes
- Relationship Requirements
  - Relationship with your DNS parent
  - Relationships with your children
- Timeline Changes

Business Model Changes

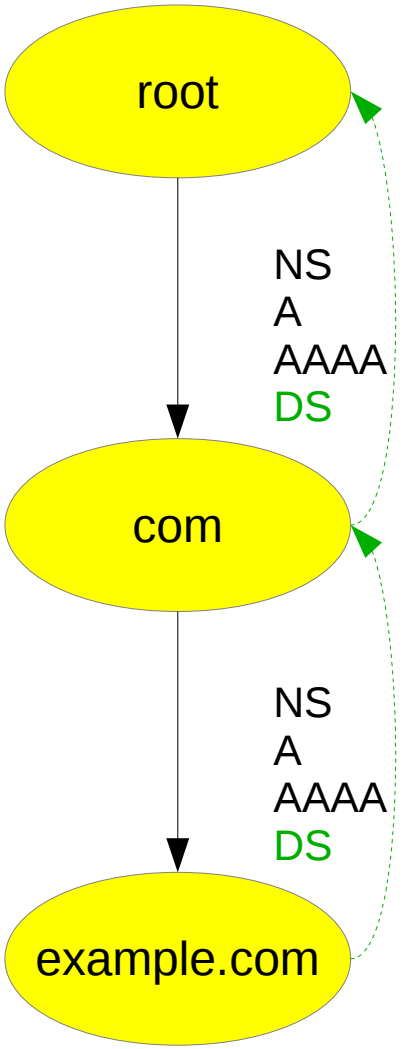
Creating a New Domain

- With DNS
  - Purchase your name, win an auction, ...
  - Use recent compliant DNS software
  - Attach to your parent
    - Business or other relationship
      - TLD → ICANN / IANA
      - Enterprise, etc → Registrar
    - Use their interface to update your NS/Glue



Business Model Changes

Creating a New Domain

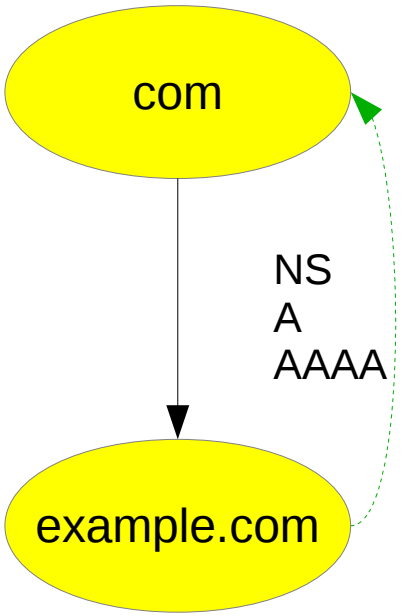


- With DNS
  - Purchase your name, win an auction, ...
  - Attach to your parent
    - Business relationship or contract
      - TLD → ICANN / IANA
      - Enterprise, etc → Registrar
    - Use their interface to update your NS/Glue
- DNSSEC Adds
  - Need to update DS records
  - Parent and interface must be DNSSEC compliant!
    - This may affect your buying and attachment decision

Relationship Changes

Relationships: With Your Parent

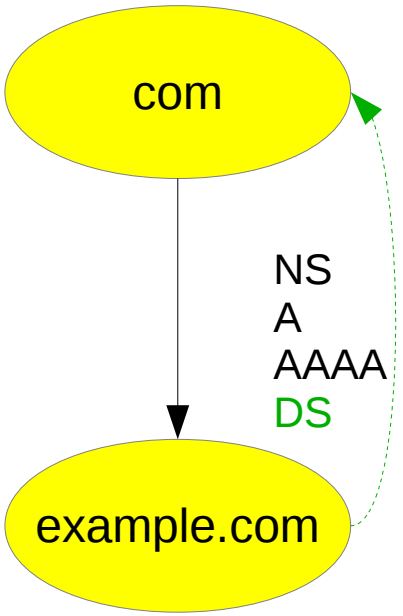
- With DNS
  - Maintain data synchronization with your parent
    - NS
    - Glue (A and AAAA)
  - Frequently while changing infrastructure
    - Likely the only time your parent data changes
    - Make sure to tell your parent
      - New or removed NS records
      - Changing A and AAAA records
    - People tend to “know” these are important
      - Because they're rare!
  - IETF's CSYNC draft automates this



Business Model Changes

Relationships: With Your Parent

- DNSSEC adds:
  - Maintain data synchronization with your parent
    - DS Records
  - When your key changes
    - When you roll your keys: tell your parent!
    - If you plan on a regular schedule
      - Make sure it's in the todo list!
      - People forget things that are periodic
  - IETF's RFC7344 (CDS) automates this



Relationship Changes
Maintaining a Domain: Testing!

- With DNS
  - Do your parent and your NS/glue records match?
  - What tools are you using?
    - Monitoring service?
    - Software?
    - Self-monitoring scripts?
      - EG: “*dig example.com NS”* vs “dig @parent example.com NS”
  - Are you going to monitor this frequently?

Relationship Changes
Maintaining a Domain: Testing!

- With DNS
  - Do your parent and your NS/glue records match?
  - What tools are you using?
    - Monitoring service?
    - Software?
    - Self-monitoring scripts?
      - EG: "*dig example.com NS"* vs "dig @parent example.com NS"
  - Are you going to monitor this frequently?
- DNSSEC Additions
  - Monitor the DS record too
    - Does your monitoring service or tool support it?

Relationship Changes

Maintaining a Domain: Testing!

Quiz!!!

- Example DS record checking using “getds”

```
--- DS records generated from querying example.com:
  EXAMPLE.COM.  3600    IN      DS      51605 8 2 (918...
  EXAMPLE.COM.  3600    IN      DS      51605 8 1 (E74...
  EXAMPLE.COM.  3600    IN      DS      31589 8 2 (CDE...
  EXAMPLE.COM.  3600    IN      DS      31589 8 1 (349...
--- DS records pulled from the parent of example.com:
  EXAMPLE.COM.  86400   IN      DS      31589 8 2 (CD0...
  EXAMPLE.COM.  86400   IN      DS      31589 8 1 (349...
```

Relationship Changes

Maintaining a Domain: Testing!

Quiz!!!

- Example DS record checking using “getds”

```
--- DS records generated from querying example.com:
  EXAMPLE.COM.  3600    IN      DS      51605 8 2 (918...
  EXAMPLE.COM.  3600    IN      DS      51605 8 1 (E74...
  EXAMPLE.COM.  3600    IN      DS      31589 8 2 (CDE...
  EXAMPLE.COM.  3600    IN      DS      31589 8 1 (349...
--- DS records pulled from the parent of example.com:
  EXAMPLE.COM.  86400   IN      DS      31589 8 2 (CD0...
  EXAMPLE.COM.  86400   IN      DS      31589 8 1 (349...

ERRORS (2):
1) The following DS record is not published in parent:
  EXAMPLE.COM.  3600    IN      DS      51605 8 1 (E74...
2) The following DS record is not published in parent:
  EXAMPLE.COM.  3600    IN      DS      51605 8 2 (918...
```

Relationship Changes

Maintaining a Domain: Testing!

- Example DS record checking using “getds”

```
--- DS records generated from querying example.com:
  EXAMPLE.COM.  3600    IN      DS      51605 8 2 (918...
  EXAMPLE.COM.  3600    IN      DS      51605 8 1 (E74...
  EXAMPLE.COM.  3600    IN      DS      31589 8 2 (CDE...
  EXAMPLE.COM.  3600    IN      DS      31589 8 1 (349...
--- DS records pulled from the parent of example.com:
  EXAMPLE.COM.  86400   IN      DS      31589 8 2 (CD0...
  EXAMPLE.COM.  86400   IN      DS      31589 8 1 (349...

ERRORS (2):
1) The following DS record is not published in parent:
  EXAMPLE.COM.  3600    IN      DS      51605 8 1 (E74...
2) The following DS record is not published in parent:
  EXAMPLE.COM.  3600    IN      DS      51605 8 2 (918...
```

Relationship Changes

Maintaining a Domain: Testing!

- Example DS record checking using “getds”

```
--- DS records generated from querying example.com:
  EXAMPLE.COM.  3600    IN      DS      51605 8 2 (918...
  EXAMPLE.COM.  3600    IN      DS      51605 8 1 (E74...
  EXAMPLE.COM.  3600    IN      DS      31589 8 2 (CDE...
  EXAMPLE.COM.  3600    IN      DS      31589 8 1 (349...
--- DS records pulled from the parent of example.com:
  EXAMPLE.COM.  86400   IN      DS      31589 8 2 (CD0...
  EXAMPLE.COM.  86400   IN      DS      31589 8 1 (349...

ERRORS (2):
1) The following DS record is not published in parent:
  EXAMPLE.COM.  3600    IN      DS      51605 8 1 (E74...
2) The following DS record is not published in parent:
  EXAMPLE.COM.  3600    IN      DS      51605 8 2 (918...
```

New?

Old?

Relationship Changes

Relationships: With Your Parent – Testing

- Testing DNS
  - Does your parent mirror your real data?
    - How often do you check?
- Testing DNSSEC
  - Is your parent's published DS for you correct?
    - How often do you check?
  - Are you testing end-to-end validation?
    - How often?

Relationship Changes

Relationships: With Your Children

- A parent is clearly the inverse of being a child
- A few important points though...

Relationship Changes
Relationships: With Your Children

- With DNS *(if you're a parent or registrar)*
  - You likely have an API for children to use
    - Unless you have a very small number of children
  - Lets them:
    - Add and remove NS records
    - Add and remove A glue records
    - Add and remove AAAA records
  - Possibly perform transfers
  - Advertise support for and use CSYNC?

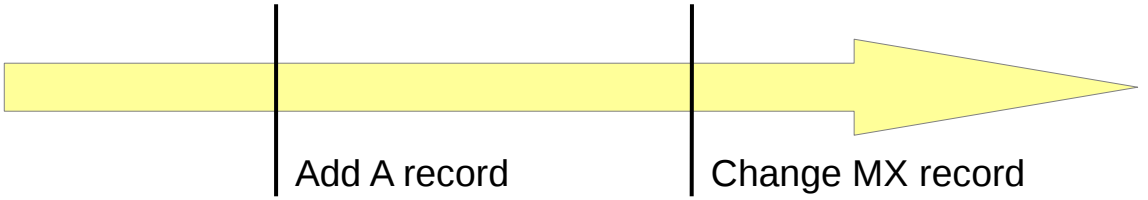
Relationship Changes

Relationships: With Your Children

- DNSSEC Adds:
  - API:
    - Add and remove DS records
  - How to transfer the new data?
    - Paste an entire DS record?
    - Fill-in form with DS parameters?
    - Paste an entire DNSKEY?
    - Fill-in form with DNSKEY record parts?
    - Who picks the DS algorithms used?
  - Advertise support for and use CDS?
- ADVERTISE YOUR SUPPORT!!!

Timeline Changes

- With DNS:

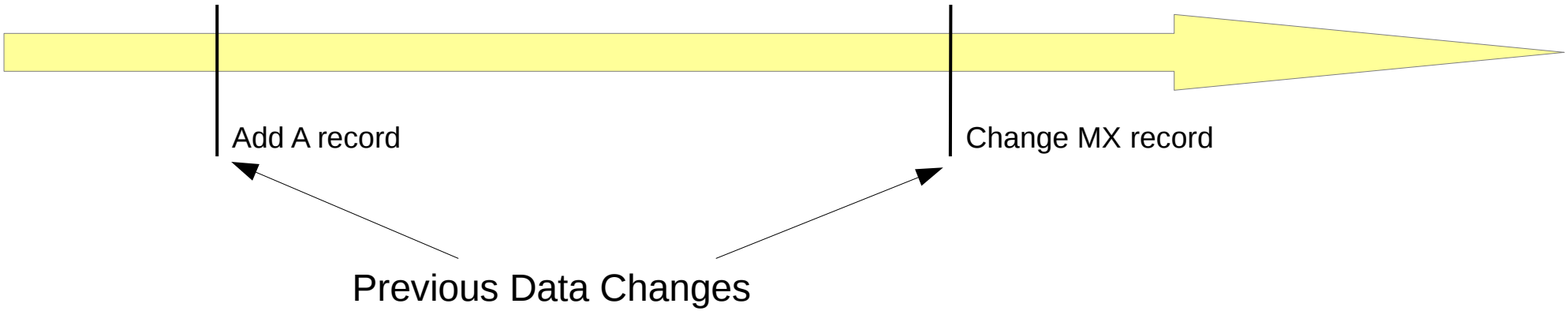


  - Data is frequently static
    - Addresses, mail records, etc
  - Sometimes it is automated:
    - Round robin records
    - Load based records
    - Generated records
      - Client or child based records
      - DNS blacklists
      - Etc
- All of these are “Fire and Forget”
  - Once served or running, little maintenance needed

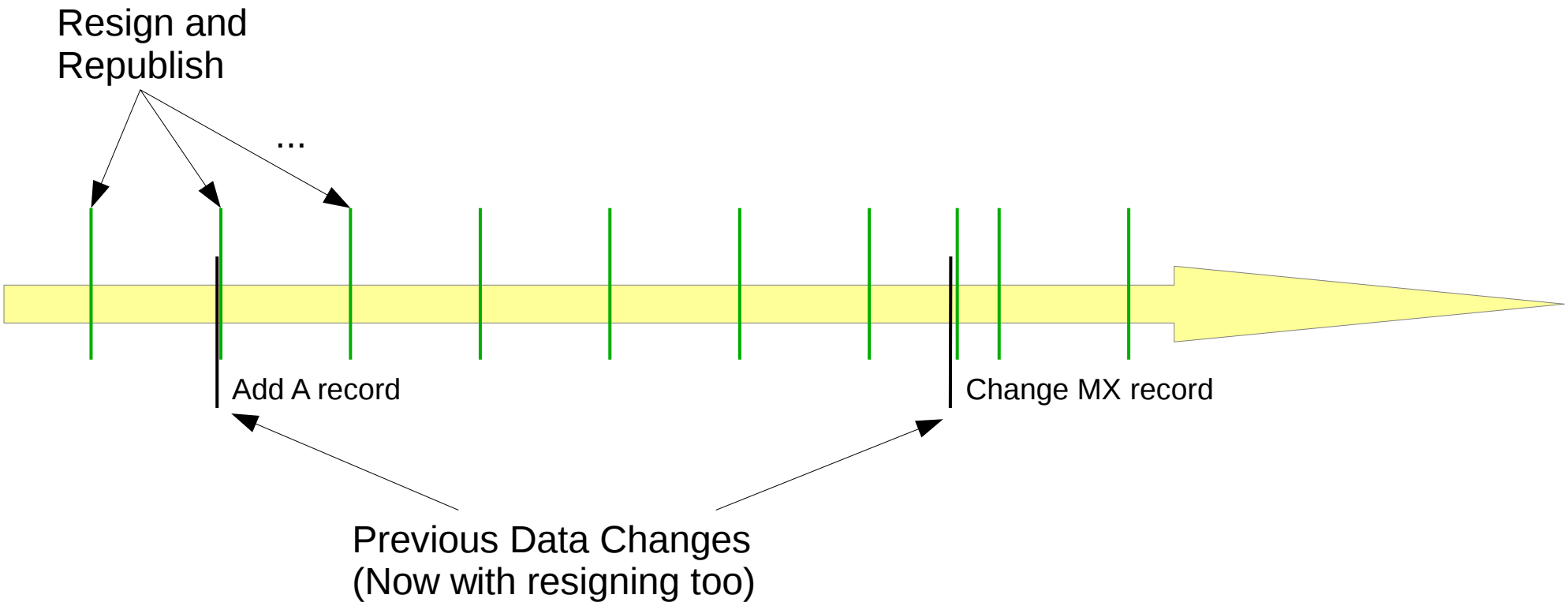
Timeline Changes

- With DNSSEC:
  - Signature records have a life time
  - DNSKEYs may require periodic rotation
- No longer “Fire and Forget”
  - Operational procedures must change!
  - Every X period of time: resign!
  - Every Y period of time: roll keys
    - Which itself is a long process, typically months

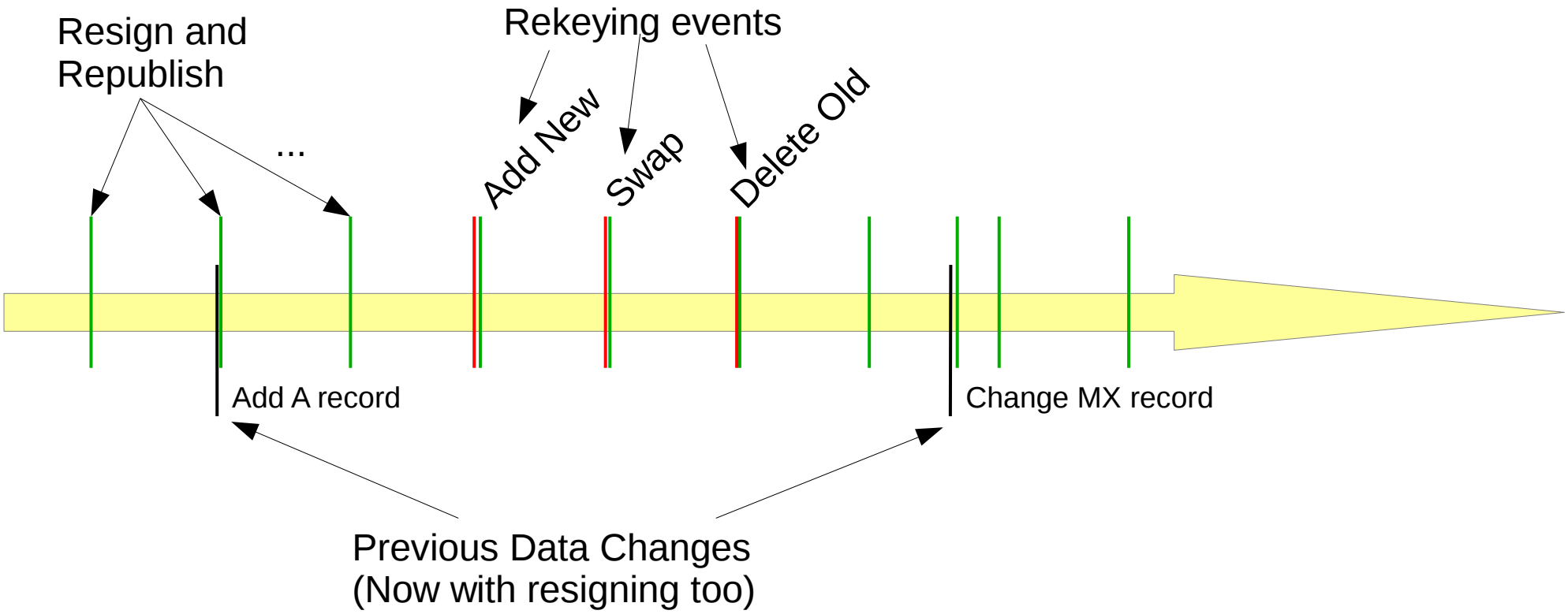
Timeline Changes



Timeline Changes



Timeline Changes



Timeline Changes
Signature Periods

- How often to resign?
  - Depends on signature length
  - Good rule of thumb: at least every: *length / 2*
  - 1 month signature → at least every 1/2 month
- Provide room for slippage
- Test and monitor your infrastructure!
    - If you fail to resign, will you notice?
    - Grace periods don't help if you don't check

Timeline Changes
Key Rolling Periods

- What are the reasons for rolling keys?
  - Key strengths
  - Good operational practice
  - Tests parent/child relationships
- So, how often should you roll keys?
  - Very situation dependent
  - Common guidances heard:
    - Roll zone-signing-keys every 3 months
    - Roll the key-signing-key annually
- Do you have a plan in place?

Timeline Changes
DANE TLS Record Changes

- Are you using DANE to secure?
  - SMTP
  - SIP
  - XMPP
  - HTTPS
- When your TLS certificate changes:
  - Will you remember to change your TLSA record?
  - Will you notice if you forget and they don't match?

Questions?

Wes Hardaker
<wes.hardaker@parsons.com>