DNS(SEC) operations

Overview

These are operational considerations when running DNS services, in the context of DNSSEC. This is in addition to the usual DNS operations best practices.

DNSSEC makes DNS a much more dynamic system. It's not fire and forget anymore.

If you don't have good DNS operational practice, DNSSEC will make your life miserable.

DNS best practice

Use a hidden SOA architecture

- Public facing servers should only be serving zones, not signing/creating/updating zone data

Place servers in geographically/topologically distinct locations (RFC2182 probably still relevant)

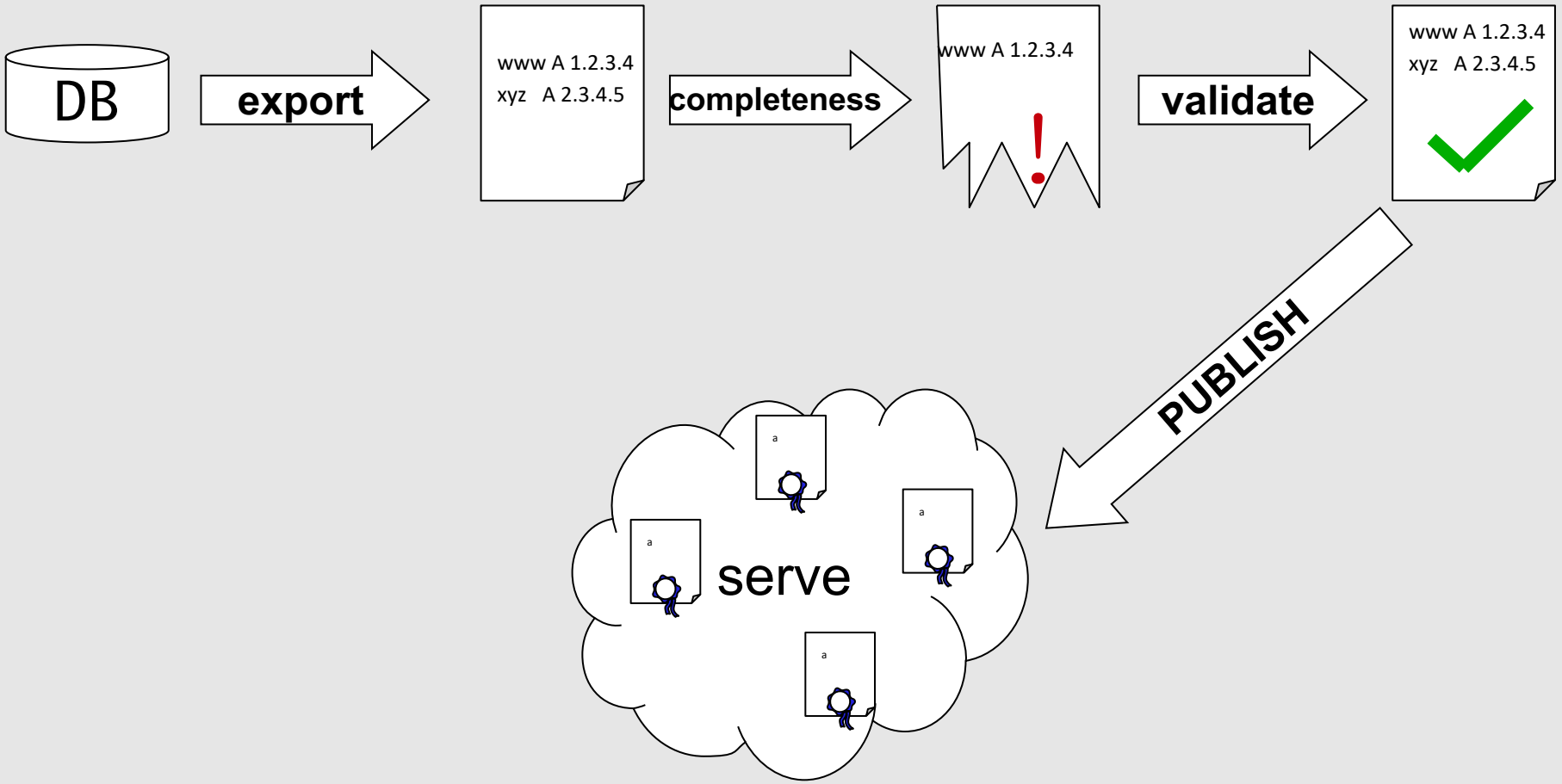
- Different cities, countries, AS

Monitoring

- Monitor your servers (health, availability/reachability)
- Monitor your zones (SOA, serial, test records)
- Monitor your zone creation / publishing process

Zone production chain

Create, validate, publish



What's new with DNSSEC ?

A number of things to watch out for:

- Authoritative server replication
  - Monitor serial number on all zones
  - If not identical, there is a problem
  - Risk of serving data signed with old key / expired sigs
- Time synchronization
  - NTP is mandatory!
  - If clock is wrong, validation can fail
  - Production of signatures with wrong date
- Signature expiration
  - Check that signatures aren't expired (or near to)
  - Have some "canary" records, but check entire zone occasionally

Possible problems

Wrong DS uploaded to parent zone, or

- Forgot to upload DS after KSK roll

Old ZSK retired too early

- Some validating servers may still have records signed with old signatures.
  - They fetch DNSKEY RRset, old ZSK isn't part of it
  - No way to validate signature!
  - RRset marked bogus -> failure!

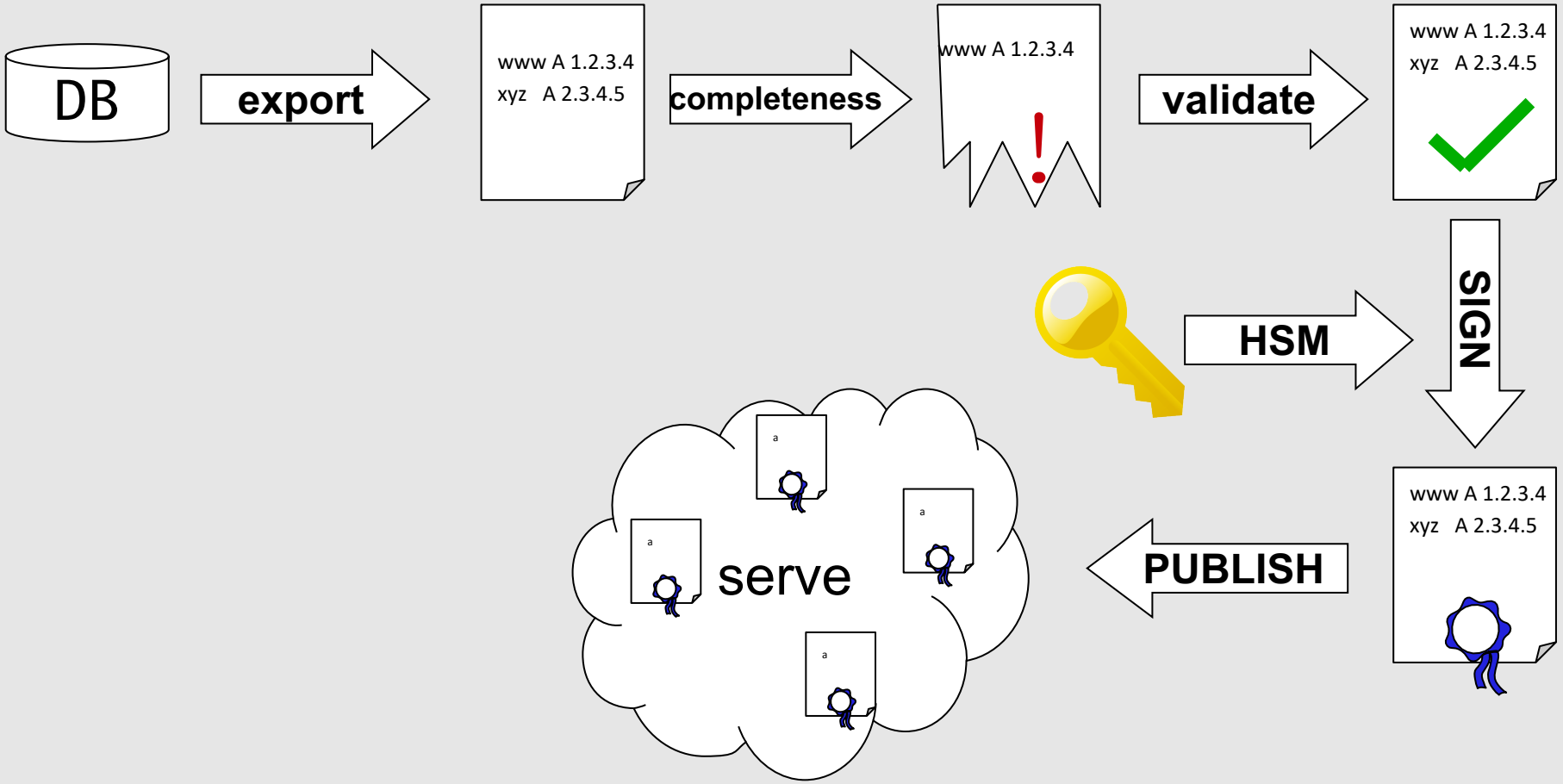
Possible problems (2)

Timing considerations

- Signature lifetime, TTL, zone refresh – all have operational impact
  - Be careful with TTL ←→ signature lifetime interaction!
  - Parent zone TTL also matters (DS publish/retire)
- Signature lifetime… how long ?
  - We'll cover this separately
  - What's the risk of too long signatures ?

Zone production chain with DNSSEC

Create, validate, sign, validate, publish, monitor



Monitoring & validating

Use your existing NMS if you have one

- If not, deploy one (Nagios, Zabbix, …)
  - Use the wonderful checksig plugin to verify signature expiration

https://github.com/ableyjoe/checksig.sh

We'll do a lab on this.

Validate your zone before publishing it

- Try http://www.validns.net

Other things to consider

Transfer zones between registrars

Automatically update DS from child DNSKEY (RFC7344)

RRset size (too many / too large signatures)

Badly configured network infrastructure

- DNS isn’t just 512/udp

Remember to remove old ZSKs