HA Deployment of OpenDNSSEC

OARC DNS Workshop

Prague, May 2010

Dave Knight

Background

Why DNSSEC?

- ICANN operates many infrastructure zones
  - IP6.ARPA, IANA.ORG, etc
- In addition to our own zones
  - ICANN.ORG et al

Why OpenDNSSEC?

- Bump in the wire signer
- Free Open Source Software
- Very active project and community
- Works with the hardware we already have
  - Linux Servers + AEP Keyper HSM

Design motivations

- Designed with root signing in mind
  - Demonstrably secure facilities and equipment
  - Fully redundant, well separated locations

IANA Testbed

- A separate effort
  - Has it's own dedicated equipment
  - Uses a signer built by Rick Lamb
    - Using some of those tools with our OpenDNSSEC setup

Facilities

Data Centres

- Terremark NAP of the Capital Region
  - Culpeper, Virginia
  - 60 miles from Washington DC
  - Meets standards for a Secure Compartmented Information Facility (SCIF)

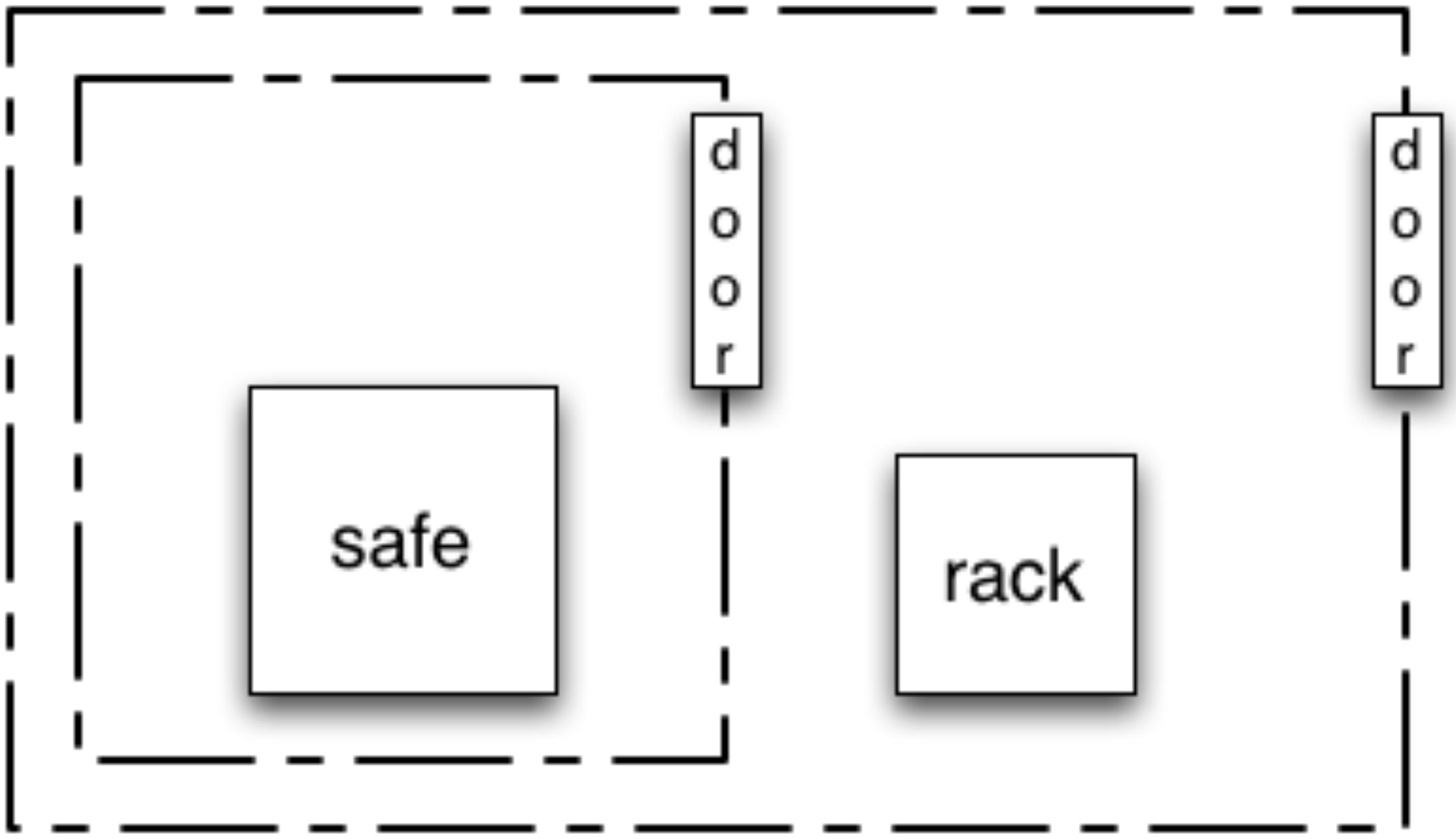
Data Centres

- Equinix LA3 El Segundo IBX Center
  - Los Angeles, California
  - 7 miles from the ICANN office in Marina del Rey

The cage

- Cage within a cage
- Located in open colocation suites
  - Should be secure, but not hidden
- Same setup at both locations
- Multiple people required to access

The cage



Hardware

The safe

- 19” rack inside a GSA Class 5 Container
- Servers and HSMs run inside
- Closed loop climate control

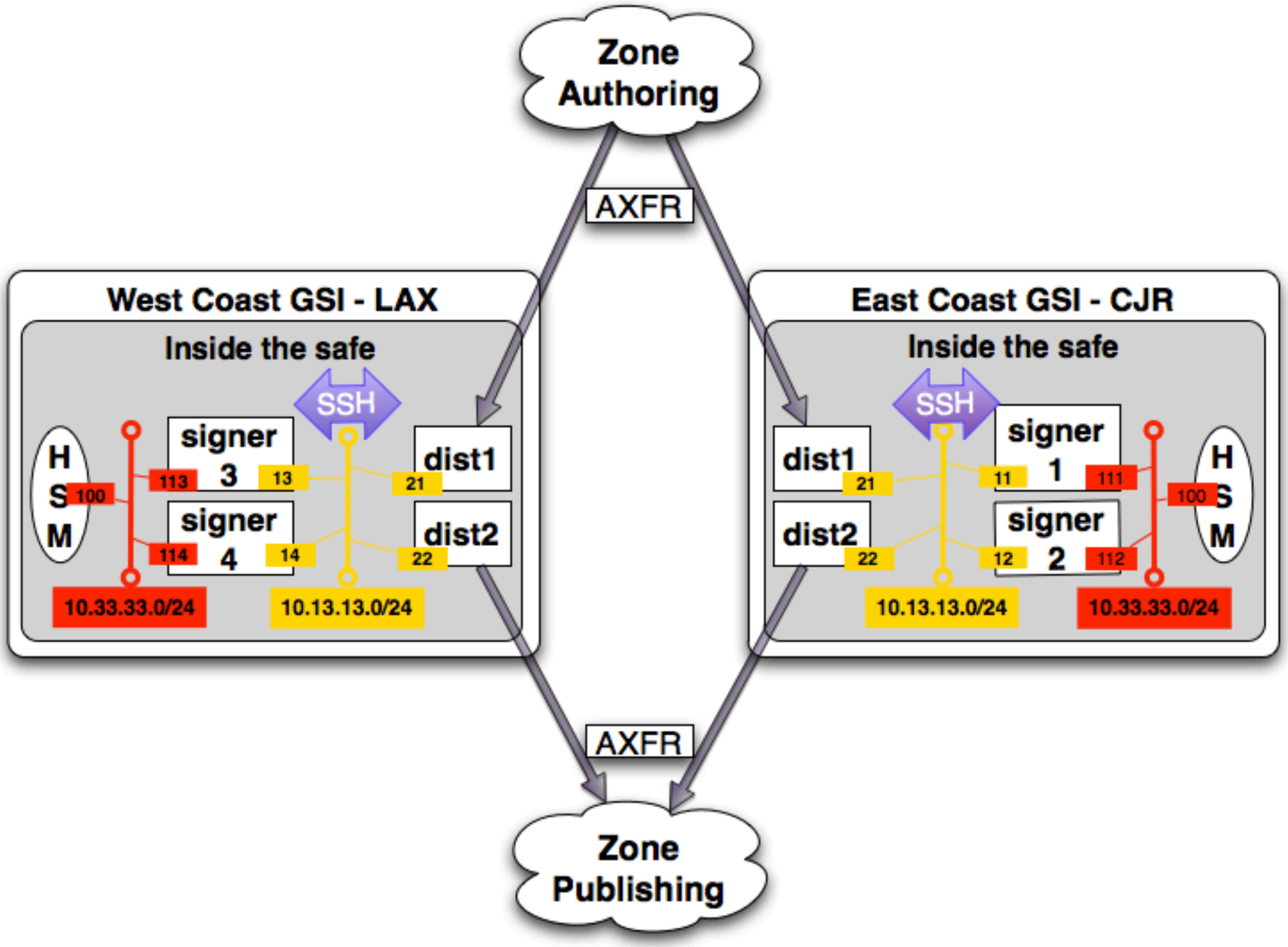
Model TSM621WXHE-12

Inside the safe

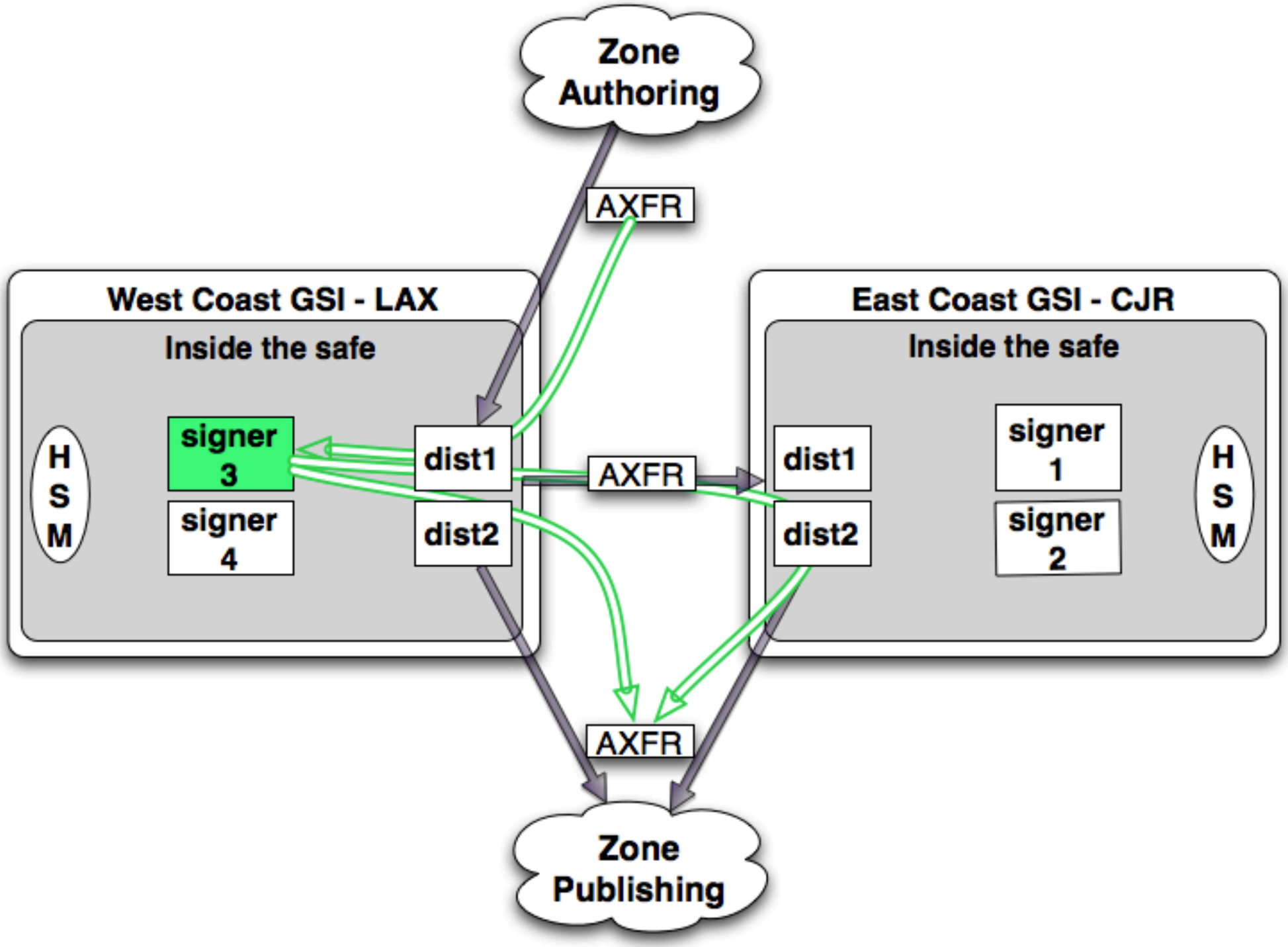
- One HSM
  - AEP Keyper
- Two Signer Servers
  - PC + Linux + OpenDNSSEC
- Two Distribution Servers
  - PC + Linux + BIND9

System

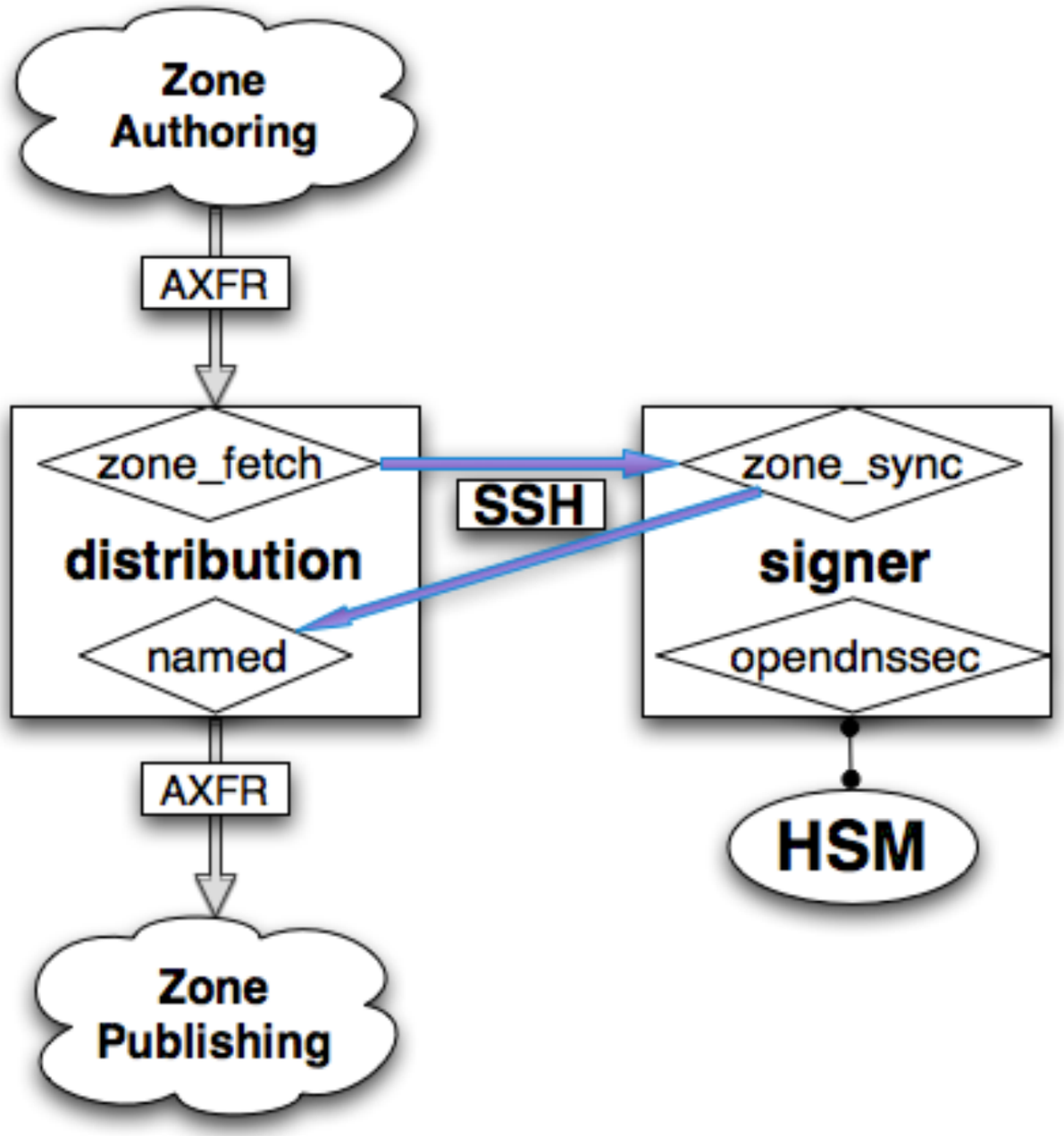
Overview


Zone
Authoring
AXFR
West Coast GSI - LAX
Inside the safe
SSH
H
S
M
100
signer
3
113
13
signer
4
114
14
dist1
21
dist2
22
10.33.33.0/24
10.13.13.0/24
East Coast GSI - CJR
Inside the safe
SSH
dist1
21
dist2
22
signer
1
11
111
signer
2
12
112
100
H
S
M
10.13.13.0/24
10.33.33.0/24
AXFR
Zone
Publishing

Active path


Zone
Authoring
AXFR
West Coast GSI - LAX
Inside the safe
H
S
M
signer
3
signer
4
dist1
dist2
AXFR
East Coast GSI - CJR
Inside the safe
dist1
dist2
signer
1
signer
2
H
S
M
AXFR
Zone
Publishing

Zone data flow



- zone_fetch
  - Pulls unsigned zone in
  - Uses AXFR
- zone_sync
  - Pulls unsigned zone in
  - Pushes signed zone out
  - Uses RSYNC over SSH

Synchronization

Signer Backup

- Script on the active signer copies the OpenDNSSEC state out to the distribution servers
  - Stop OpenDNSSEC
  - Make a tarball
  - Rsync that out
  - Start OpenDNSSEC

Signer Restore

- Manually copy the latest backup to the target signer and run the restore script
  - Makes sure that OpenDNSSEC isn't running
  - Unpacks the tarball
  - Starts OpenDNSSEC

HSM Backup

- Keys are created at zone initialization
  - Ongoing backup is not needed
- Keys can be copied using smart cards or moved securely across network using pkcs11-backup
  - pkcs11-backup written by Rick Lamb
  - Keys are encrypted on the wire using a key shared manually with smart cards at HSM initialization

Failover

Failover within a site

- Both signers use the same HSM
  - Backup/Restore scripts copy over Keyper's keymap database
- Copy the OpenDNSSEC state

Failover between sites

- Copy keys from the HSM where they were created to the other
  - Done when keys are created at zone initialization
- Copy the OpenDNSSEC state
- Invert the master/slave relationship of the distribution nameservers

Common operations

Zone initialization

- Add a new zone on the active signer, create 2 years of keys in advance
- Copy the new keys from the active HSM to the inactive one at the other site
- Add the zone to the configuration of the distribution servers

Key Management

- OpenDNSSEC manages ZSK rollover
- KSK rollover is a manual operation
- Periodic manual exercise to create more keys

Zone removal

- Tell OpenDNSSEC to drop the zone
- Manually remove keys from the HSM

Questions?

dave.knight@icann.org