So you want to do DNSSEC...

.NA®’s First Experiences With the PCH Signing Platform

Dr Eberhard W Lisse

Namibian Network Information Centre (cc)

ICANN 42, Dakar
Background

- *Old* ccTLD
  - Third in Africa (1991)
  - Continuous Management
- Shared Registry
  - CoCCATools
- **Serious** Anycasting
- Signed Before the Root
  - Key Generated with BIND9’s *dnssec-keygen*
- 1 Production Zone signed (lisse.NA).
CoCCATools

- Open Source
- Active Development
- Very Stable
- IPv6 Compatible
- **Automated**
  - Backup
  - **Zone Generation**
- No Key Management Support
  - Yet
  - DS Records Manually Inserted
Perl Script

- Takes CoCCATools’ Zone
- Signs with `dnssec-signzone`
- `scp` to Master
  - `gzip` and Archives Each Version
- Does **not** reload Master
- Runs hourly via `crontab`

Master

- Picks up, installs and reloads zone
- Notifies Slaves
Perl Script

- Takes CoCCATools’ Zone
- Does not sign
- `scp` to Master
  - `gzip` and archives each version
- Does not reload Master
- Runs hourly via `crontab`

Master

- Picks up, installs and reloads zone
- Does not sign
- Notifies Slaves (PCH and others)
Hidden Master on the Register Portal
  - BIND9

CoccaTools
  - Generates Zone File
  - Reloads BIND9
    - Notifies Master (PCH)
  - Runs hourly but **not** via `crontab`
Promoted from Slave to Master
  - Some coordination required

AXFRs
  - from Hidden Master (Portal)
  - via TSIG key distributed by signed/encrypted GPG email

Signs Zone on Verified Platform

Notifies Slaves
  - AXFR
Summary

Lessons Learned

- Learning Curve
  - TSIG
  - RFTM!
- Process itself
  - Easy!
  - It Just Works!
Summary
5 Easy Steps

1. Set Up Hidden Master and Configure it
   - To notify PCH; and
   - To allow AXFR from PCH

Using TSIG

2. Coordinate with PCH
   - Delegate to PCH
     Additional benefit of Anycasting

3. Add DS Records to Parent Zone

4. Wait for Signed Zone to Show Up

5. Promote PCH to Master
   - Coordinate with PCH, Slaves and former Master
Next Steps

Uptake

- Market DNSSEC
  - Increase Awareness
- Once/If Critical Mass Achieved
  - Consider Repatriation (from PCH)
    - OpenDNSSEC
    - Key Generation Hardware
    - Secure Facility
- Consider Cost
Thank You

Lawrie’s Law

- Vicky Shrestha, PCH
- Robert Martin-Legène, PCH
- Peter Losher, ISC