DNSSEC for humans

João Damas
ISC

ICANN 39, Cartagena de Indias,
Colombia. December 2010
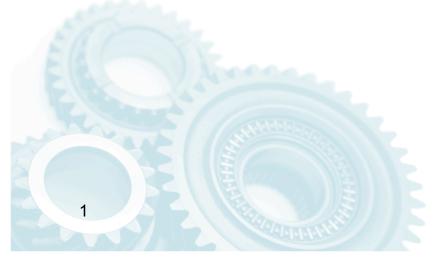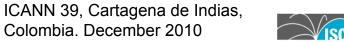
Overview

- DNSSEC for mere mortals: BIND 9.7
  - DNSSEC for humans now
  - DNSSEC for humans, even better

- A hint of BIND 10

ISC

BIND 9.7 - DNSSEC for humans

- Automation
- Support for HSMs (aka PKCS#11)
- Easier dynamic DNS
- Performance improvements
- New algorithm support
- For recursive servers
  - Automated trust anchor maintenance
  - Simplified DLV configuration

BIND 9.7 - DNSSEC for humans

- Automation
  - Fully automatic signing of zones

- Automated trust anchor maintenance
  - recursive servers (RFC 5011)

BIND 9.7 - DNSSEC for humans

- Support for HSMs
  - Talks to Hardware Security Module using PKCS#11
  - includes tools to manage keys in the HSM

ISC

BIND 9.7 - DNSSEC for humans

- Easier dynamic DNS
  - includes automatic key generation and configuration
  - includes tools to simplify manual work

BIND 9.7 - DNSSEC for humans

- Performance improvements
- New algorithm support
  - SHA2 (like the root zone)
  - GOST (for those who need it, soon)

BIND 9.7 - DNSSEC for humans

Other new features improving security

- DNS rebinding attack prevention
  - http://en.wikipedia.org/wiki/DNS_rebinding

DNSSEC for humans, even better

- To be included:
  - automatic key management
    - creation/revokation/rollover
  - bump-in-the-wire signing
- YOUR REQUEST HERE
  - talk to us

ISC

A hint of BIND10

- BIND 9 has been around for 11+years
- Time for a refresh
  - new OS, new hardware, new use models
- BIND 10
  - New modular approach (pick the bits you need, slide in your own)
  - new configuration model
  - cluster support
  - Coming to a server near you in 2011

ISC

Making it better

http://www.isc.org/software/bind/new-features/9.7

Always seeking input, requests for missing features, things you would like to have, things you would like to be different.

ISC

Questions?
joao@isc.org