Evolution of DNSSEC in BIND9

Early stages

- BIND 9.0 already supported original DNSSEC (RFC 2535)

- bundled with tools to
  - create keys
  - sign and verify zones with keys

  - tools have evolved to track evolution of DNSSEC

The DO bit

- Additional flag in EDNS(0) additional flag field
- Introduces the requirement to support ENDS(0) in order to do DNSSEC
- Interpretation
  - –apparent intention was to add flag to request DNSSEC
  - –Actual implementation was to signal “understand DNSSEC”

Modern DNSSEC

- RFC 3845 (NSEC replaced NXT)
- RFC 3658 introduced DS record
  - –BIND 9.4

- Later introduced NSEC3
  - –BIND 9.6

Islands of security

- Concept to allow early deployment of DNSSEC
  - Introduces the idea of trust anchors
  - Allows manual configuration of multiple DNSSEC keys as starting points to validation
  - Defines sub-trees where validation is possible

Deployment aids - DLV

- DLV introduced in BIND 9.4
  - parallel trust tree to allow for DNSSEC registration and validation
- Automation of trust anchors management
  - allows for better scaling of islands of security
  - define possiblity of local policy

BIND 9.7 - Operational features

- first step in operational automation
  - continuous signing
  - Will prevent expiration of signatures
  - will sign dynamic zones
  - will roll keys according to declared policy

Policy

- basic policy description
  - extended format for Key files

```
; This is a zone-signing key, keyid 49563, for isc.org.
; Created: 20120605005218 (Tue Jun  5 08:52:18 2012)
; Publish: 20120605005218 (Tue Jun  5 08:52:18 2012)
; Activate: 20120605005218 (Tue Jun  5 08:52:18 2012)
isc.org. IN DNSKEY 256 3 5
AwEAAbBT0JlGUY421zAYrdVLAhk83sKgnhof7OSuS8xX8BVfBXzNZ8B
W 3CFktU8QYjen91VMDCvtoTHHPkM1b
+YB3WkTmyh9k7J1UZcT0BCuAdTV 3nZ/LhJLjBuKbFtw3sA
+U7v3bTYjfzSCfApk/4WiDoTXX30djAvXLLWO RHmJj/15
```

BIND 9.8

- Support for GOST algorithm

BIND 9.9

- introduces **inline signing**
  - accepts an unsigned zone on one side
  - signs the zone internally
  - and provides it to other DNS server in the DNS publication workflow

  - Allows for introduction of DNSSEC in a contained system, with minimum disruption to existing publication workflows

The future - a glimpse

- BIND 10 and BIND 9 to share key management system
  - under development

Questions?