Bond Internet Systems

DNSSEC signer diversity

João Damas

State of affairs

- One commercial solution

- One Open Source solution in beta

  - primarily focused on the DNSSEC technology

- a few toolsets (e.g. zkt)

- BIND 9.7

Goals

- Increase diversity by developing new DNSSEC signing software to meet some requirements:
  - Open Source
  - Minimal disruption to current DNS edit/manage/publish cycle
  - Act as a black box or allow curious minds to look inside
  - be independent of the DNS server used

Inline Signer

- Joint project between Bond I.S. and Afilias

- Intended release date: Spring 2010

  - wanted to have working code available today but...

- Open Source

- v1 is based on ldns

Inline signer

- Can run on same system as DNS servers or on a separate system

- Support HSM key storage but not mandatory

- Human readable configuration

  - attribute:value pairs rather than XML

- Interactive and scheduled actions

Inline signer

- discrete pieces
    - module in charge of applying user specified policy (or defaults) and overall control
    - signing engine
    - publisher
    - control module

Inline signer

- Leverages work done by others
  - OpenHSM as an option
  - ldns
  - Previous experience with other software

Questions?