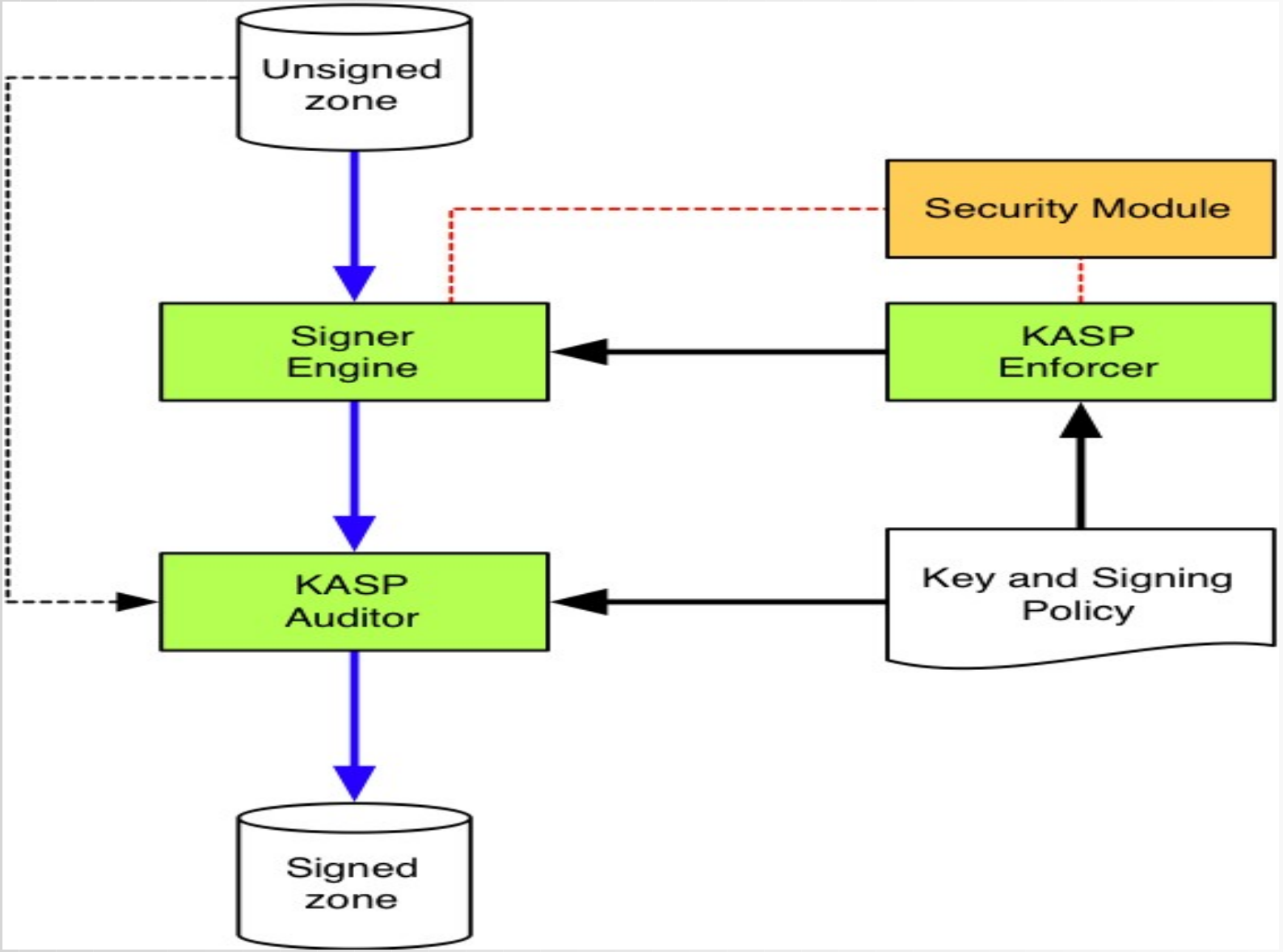
DNSSEC deployment in NZ

Andy Linton
asjl@lpnz.org

.nz is our home

http://www.opendnssec.org/



.nz is our home

The Features of OpenDNSSEC

- No manual management is needed (after first configuration)
- Works with all different versions of the Unix operating system
- Multiple zones with shared or individual policies
- Each policy specifies a set of key and signature settings
- Handle zone sizes ranging from a few RRs to millions of RRs
- Unsigned zone file in and signed zone file out.
- Supports RSA/SHA1 signatures – ready for future algorithms (e.g.RSA/SHA2,GOST)

The Features of OpenDNSSEC

- Denial of existence using NSEC or NSEC3
- Automatic key generation in HSMs via the PKCS#11 interface
- Option support for sharing keys between zones
- Automatic key rollover
- Possibility of manual key rollover (emergency key rollover)
- Automatic zone signing using HSMs via the PKCS#11 interface
- Auditing of the signing process and result
- BSD license

Issues that drive the policy

- Cannot turn DNSSEC off (yet)
- Keys - New, important things to manage
- Expectations of security
- Few properly understand DNSSEC
- Introduces new costs

.nz is our home

Registrars

- New obligations on registrars
  - Cannot go back once DNSSEC introduced
  - Cannot just restore a backup - more complex
  - Security standards for managing keys
- If registrar holds private keys…
  - Do keys move with change of registrar?
  - Must registrar cooperate with key rollover?
  - Must keys be placed in escrow?
  - What if they won't cooperate?
- How is registrar failure handled?

.nz is our home

Registrants

- Once DNSSEC is enabled, things change
  - Cannot just change their mind
  - Restricted in registrars they can use/move to
- If the registrant hold private keys
  - Must they go via registrar to send to registry?
    - Supports current model of many TLDs
    - Will registrar be the weakest link?
  - Can they send keys direct to registry?
  - That way keys can follow the registrant
  - Breaks current model of many TLDs
- What happens if their keys are compromised?

.nz is our home

Technical Considerations

- How often will TLD allow key rollovers in delegated domains?
- Will TLD insist on:
  - Min/Max key size?
  - Min/Max signature lifetime?
  - KSK -> ZSK configuration?
  - Min/Max number of KSKs?
- DNSSEC equivalent of lame delegations?

.nz is our home

Education

- Whose responsibility?
- Just education or promotion as well?
- What resources do registrars need:
  - Off-the-shelf policies on key management, signatures etc?
  - List of supporting tools?
  - Support in existing toolkits?
- Do we test registrar knowledge?
  - Special DNSSEC accreditation?

.nz is our home

Pricing

- Undeniably means an increase in costs
- How does this fit with cost recovery?
  - Policy adopted by many TLDs
- Charge more?
  - Split out costs for those that use DNSSEC?
- Charge the same?
- Charge less?
  - Drive up adoption

.nz is our home