nominet

DNSSEC and Signing .uk

28/05/2009

Brett Carr

Introduction

- DNSSEC Refresher
- Current .uk infrastructure
- Overview of opendnssec
- New .uk infrastructure
- Challenges in signing second level domains

DNSSEC Refresher

- Provides authentication of DNS responses
- Provides proof of non existence
- New records

DNSKEY	Public Key
RRSIG	Signature of Resource Record Set
NSECShows next record in zone	
NSEC3	Shows next record in zone (hashed)
DS	In parent, provides secure delegation.

- Howto (simplified)
  Create keys (dnssec-keygen)
  Sign zone (dnssec-signzone)
  Make keys available or
  Upload DS records to signed parent.
- Critical
  Keep private keys safe and secure.
  Consider and document keyrollover procedures
  Secure methods for talking to parents/children

Current .uk infrastructure

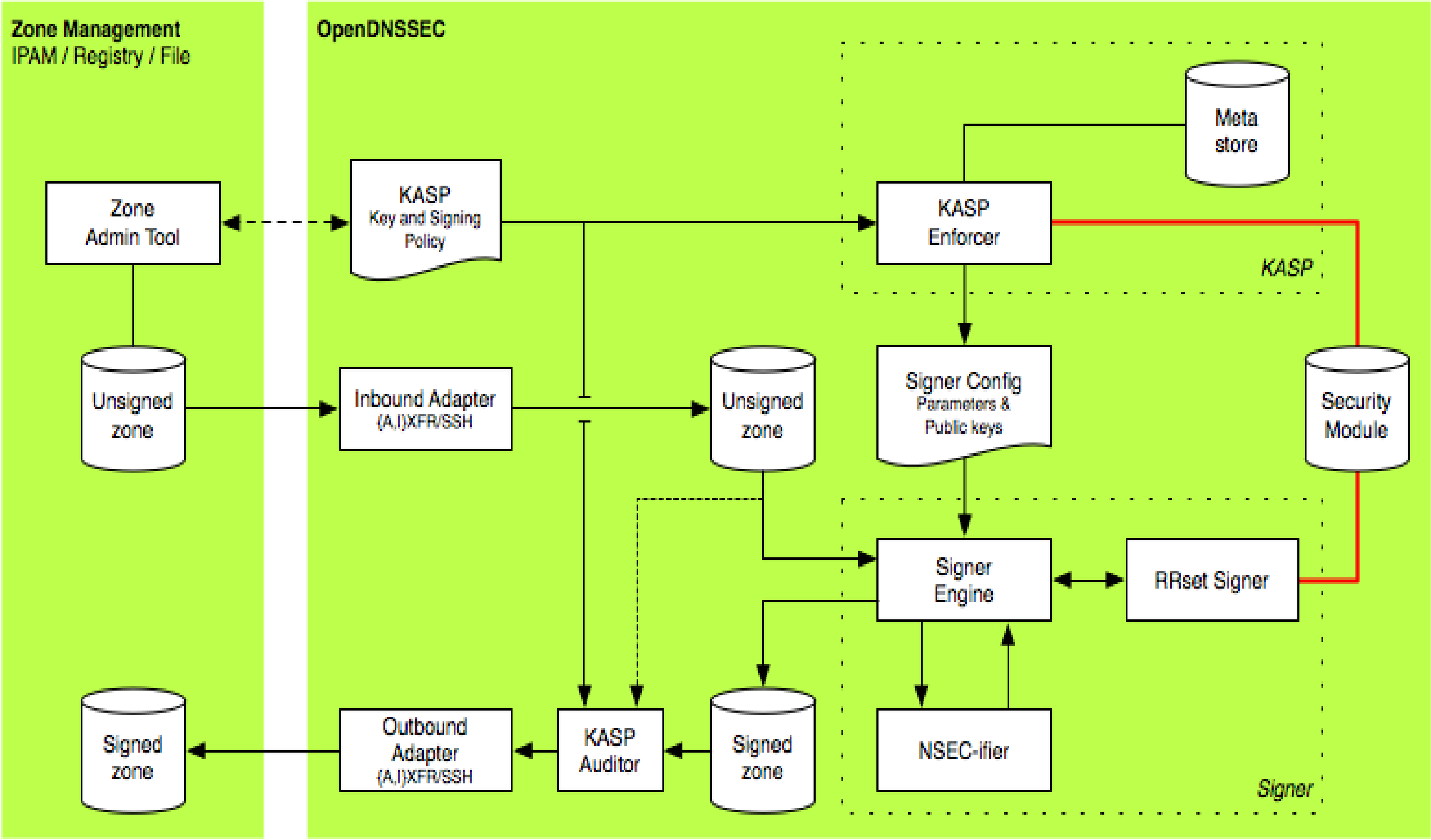
- Hidden Master
- Zone under manual edit/control
- AXFR to public master (ns1.nic.uk)
- AXFR to other nameservers (ns2-7,a-d).nic.uk

opendnssec

- Simple turnkey solution for dnssec
- Easy setup and configure
- Set Key and Security Policy (KASP):
  Key algorithim type
  Key Length
  Signature lifetime
  Keyrollover parameters
- Point it at your zonefile(s)
- Load the signed output into your nameserver
- Publish your key and/or upload DS to parent.
- Supports external HSM's with PKCS11 interface
- SoftHSM for testing/development included

nominet

opendnssec



opendnssec

- Developed by:
  NLNetlabs
  .SE
  Nominet
  Surfnet
  Kirei AB
  John Dickinson
- First beta release at IETF Stockholm in July
- http://www.opendnssec.se

New .uk Infrastructure

- Hidden Master
- AXFR to Signer running opendnssec with HSM
- AXFR to public master (ns1.nic.uk)
- AXFR to other nameservers (ns2-7,a-d).nic.uk

.

Other tasks

- Education and outreach to second level domains
- Publicise to internet community
- Check/change procedures related to information exchange
- Publish the public key(s) in IANA ITAR

Second Level Domain Challenges

- Second level domains are MUCH larger
  uk 6 Kilobytes
  co.uk 400 Megabytes
- Second level domains are restricted from external AXFR
- Second level domains are updated using dynamic updates

- Size means opt-in (RFC5155) is a requirement
- AXFR Restriction means NSEC3 (RFC5155) is a requirement
- Dynamic updates mean that continous signing is a requirement
- Update to registry systems for DS records

Questions/Comments