.eu DNSSEC deployment

DNSSEC Workshop – ICANN Meeting Brussels
Wednesday 23 June 2010

Peter Janssen
Technical Manager
EUR*id* vzw

DNSSEC Implementation

➢ Registrar *uploads* DNSSEC keymaterial
- ❑ EPP (RFC 4310)
- ❑ Registrar web application

➢ NSEC3/OPT-OUT

➢ Support ZSK/KSK

➢ Dynamic Update Process

New domain

Domain name		(*)
Registrant		(*)
Billing contact	c479	(*)
Onsite contacts	1.	(1) ⊕
Technical contacts	1. ▼	(1) ⊕
Name server groups	1.	⊕

Name servers

	Server name	IP address	
1.			⊕

Keygroup

Keys

	Keytag	Flags	Protocol	Algorithm	Public key	
1.		▼	3	▼		⊕

KSK
ZSK

DSA-SHA1 (3)
DSA-SHA1-NSEC3 (6)
RSA-SHA1 (5)
RSA-SHA1-NSEC3 (7)

Passphrase   *)

[OK] [Clear]

(1) At least one technical or onsite contact required.

Timeline

- ➢ **9 June 2010**
  - ❑ Accept DNSSEC keymaterial through registration system

- ➢ **16 June 2010**
  - ❑ Sign .eu zone
  - ❑ DS records inserted in .eu zone

- ➢ **15 July 2010**
  - ❑ Publish .eu DS record in root zone

2.4. Including DS RRs in a Zone

The DS resource record establishes authentication chains between DNS zones. A DS RRset SHOULD be present at a delegation point when the child zone is signed. The DS RRset MAY contain multiple records, each referencing a public key in the child zone used to verify the RRSIGs in that zone. All DS RRsets in a zone MUST be signed, and DS RRsets MUST NOT appear at a zone's apex.

A DS RR SHOULD point to a DNSKEY RR that is present in the child's apex DNSKEY RRset, and the child's apex DNSKEY RRset SHOULD be signed by the corresponding private key. DS RRs that fail to meet these conditions are not useful for validation, but because the DS RR and its corresponding DNSKEY RR are in different zones, and because the DNS is only loosely consistent, temporary mismatches can occur.

Predelegation tests

- For every DNSKEY key material (published as DS RR in the .eu zone)
  - DNSKEY should be present in child zone
- Coherence check
  - All (child) name servers should contain "identical" zone
    - SOA
    - NS RRset
    - DNSKEY RRset
- Several re-checks
- Notification system with "issue" report
  - Registrar Web
  - EPP (comand/dynUpdateStatus)