ROMANIA TOP LEVEL DOMAIN

INSTITUTUL NAȚIONAL
DE CERCETARE - DEZVOLTARE
ÎN INFORMATICĂ

DNSSEC Implementation

RONOG

11 October 2016

.ro Registry - ROTLD

- ROTLD is a department of “National Intitute for R&D in Informatics – ICI Bucharest”
- ICI is a state-owned company, coordinated by Ministry of Communication and for Informational Society
- In 1992, ICI operated the first connection to Internet from Romania
- It was the first ISP in Romania for research and education organizations, starting in 1992
- February 26, 1993: IANA delegated the authority to register .ro domain names to ICI Bucharest

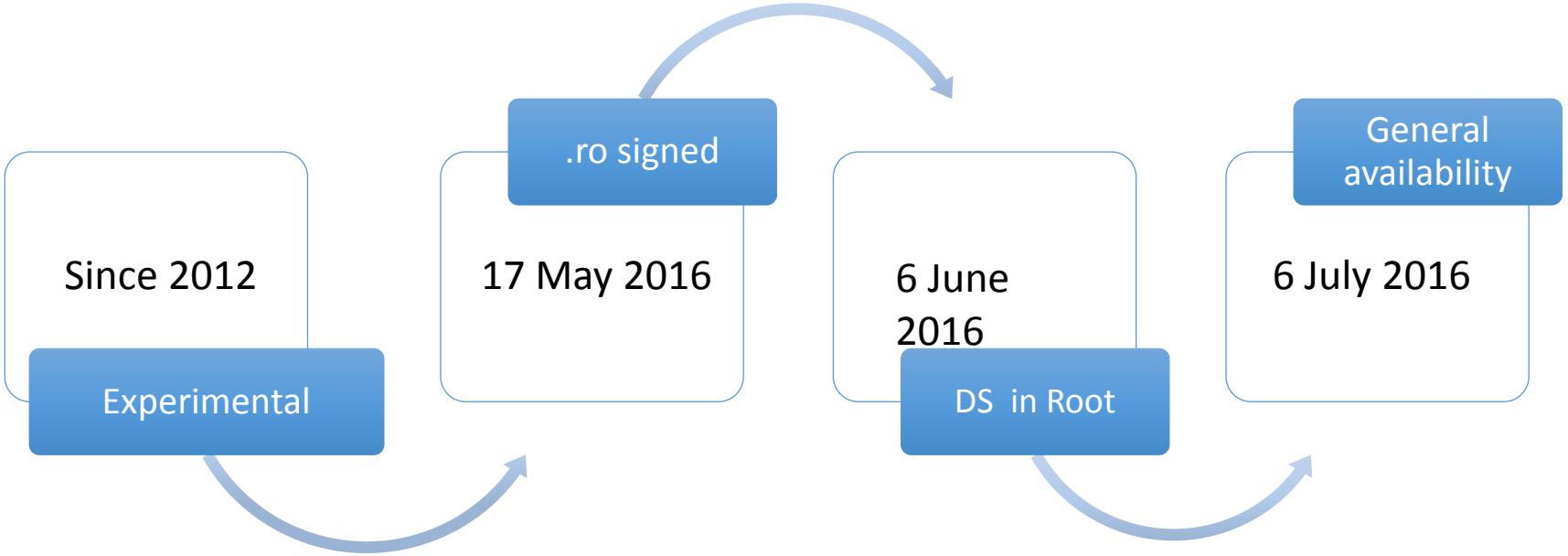
.ro Registry - ROTLD

- .ro is an “open” TLD, any person or entity is permitted to register
- Registration on a “first come - first serve” principle
- At present there is only one-time payment for registration, no renewal fee (need to be changed)
- Direct registration or using one of more than 90 Registrars
- Registrars can register in real time using APIs (EPP or REST)

Registered .ro domains

Evoluția numărului de domenii ".ro" înregistrate în perioada 1993-2015

.ro DNSSEC Timeline



.ro DNSSEC Experimental Phase (1)

- Starting in late 2012
- Getting familiar with DNSSEC technology, training and courses at RIPE NCC and IIS (.SE registry)
- First TestBed operational in 2013, working with BIND and in house developed key management software
- Tests with complete chain of trust using reverse and ENUM zones
- Decided to also test different signing software solutions

.ro DNSSEC Experimental Phase (2)

- Second TestBed with OpenDNSSEC v1.4 with SoftHSM
- .ro zone is dynamically updated
- At that time OpenDNSSEC didn’t support that so problems encounter
- BIND was the next choice with “auto-dnssec maintain”
- Developed a brand new key management system using OpenDNSSEC backend and Java

.ro DNSSEC Experimental Phase (3)

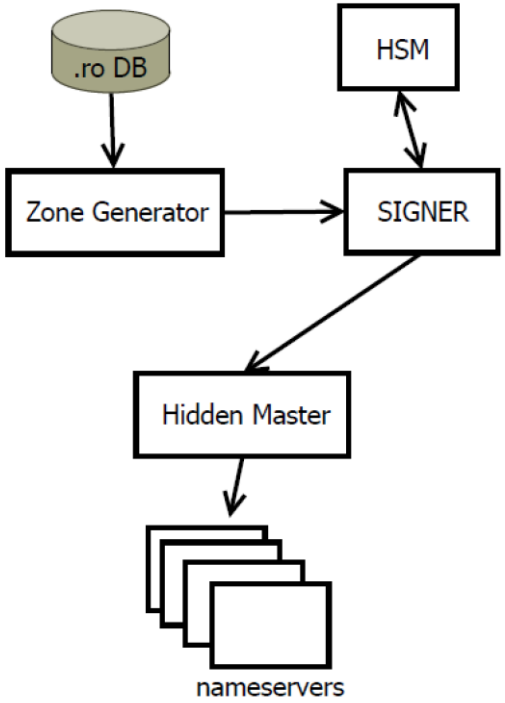
- HSM devices acquisition (Thales nShield Connect+) in 2015
- BIND officially support this HSM in native PKCS#11 mode
- Redundant deployment using Security World, easy backup of RFS, unlimited key storage, load sharing of cryptographic operations
- Phisically secured

.ro DNSSEC Experimental Phase (4)

- Upgraded registration system to support DNSSEC (databases, middleware, REST, EPP, frontend apps)
- Audit the network infrastructure (especially firewalls).
- Continuous service monitoring and zone validation (Nagios, Cacti and other custom tools)

.ro DNSSEC Experimental Phase (5)

- Final design: BIND with HSM + OpenDNSSEC backend + in house key management software



.ro DNSSEC Experimental Phase (6)

- Why it took so long:
  - Initially not a high priority project
  - Lack of a dedicated team until 2015
  - Intermittent work periods
  - Tested multiple software solutions
  - Delayed acquisition procedures
  - Minimize the risks of errors when the system is in production

.ro DNSSEC in production

- ZSK 1024 bits RSA-SHA256 (rolled at 90 days)
- KSK 2028 bits RSA-SHA256 (rolled every year)
- NSEC3, OPT-OUT signing
- 30 days RRSIG validity
- Allowed DS record algorithms: 3, 5, 6, 7, 8, 10, 12, 13, 14 and hash type 1 and 2
- First signed domain was rotld.ro

.ro DNSSEC in production

- Currently very low used
- Around 150 signed domains (less than 0.02% from 890.000 total .ro domains)
- Raise awareness among community
- Organize workshops for registrars and registrants

.ro DNSSEC

Thank You !

Ing. Catalin LEANCA

catalinl@rotld.ro

http://www.rotld.ro