.ORG DNSSEC TRANSFER TESTS LESSONS LEARNED

Olafur Gudmundsson

Shinkuro.com

Goal: Demonstrate the ripple-free DNSSEC transfer process works

- ORG Registry Operator Afilias supported on behalf of PIR.
- Shinkuro developed the tests and ran the process
- Names Beyond Registrar and DNS operator
- DynNet Registrar and DNS operator.
- Sparta participated as DNS operator.

- Report on process will issued soon

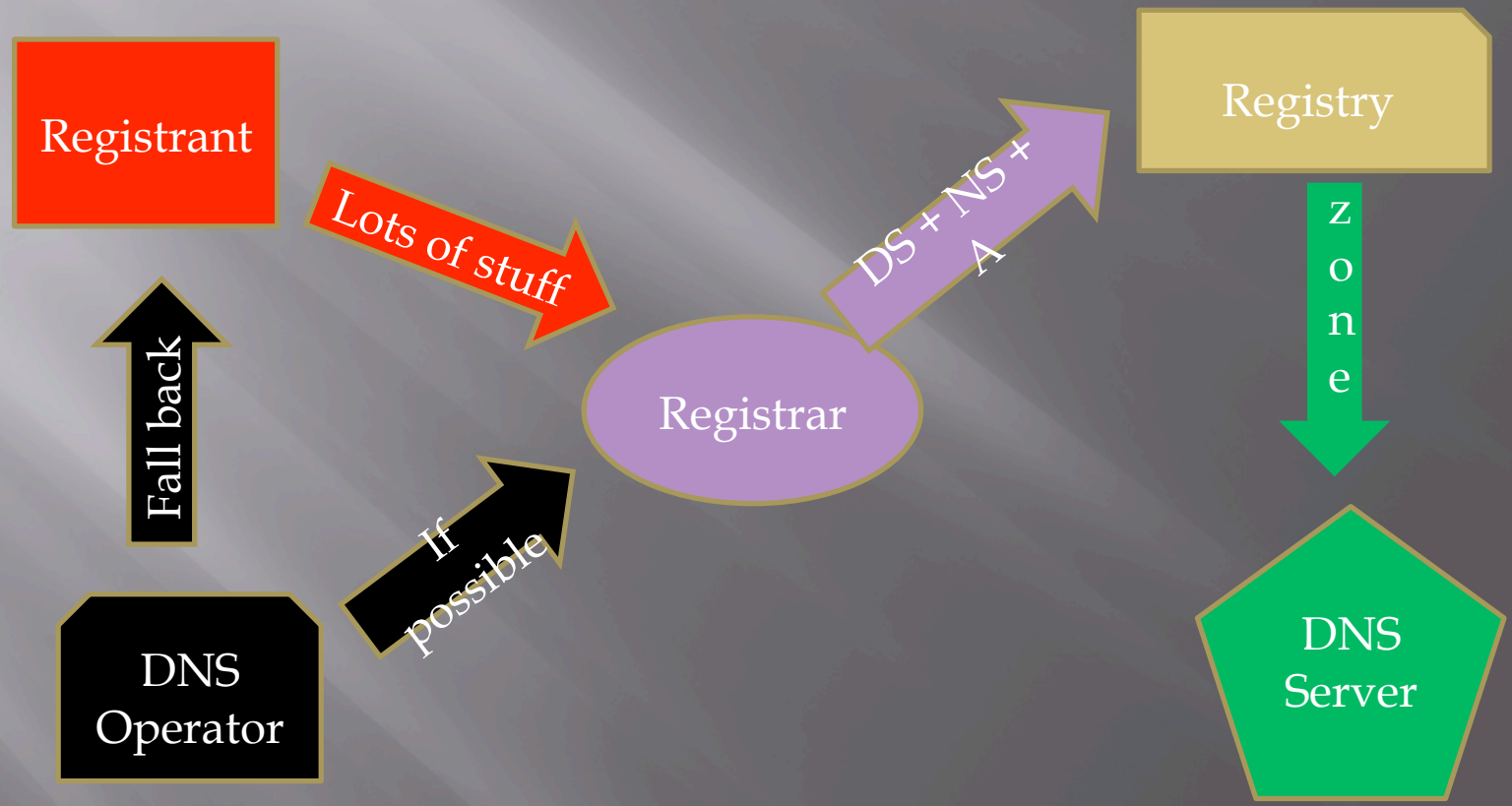
Background: Roles

- *Registry*: maintains a database and publishes DNS
- *Registrar*: Maintains customer relationship with Registrant
- *Registrant*: The holder of a domain name
- *DNS Operator*: The party that operates DNS on behalf of Registrant.

Ripple free transfer process

- Goal:
  - No DNS lookup failures,
  - No DNSSEC validation errors
- Approach:
  - Pre-Publication of DNSSEC information.
  - Wait for information to disseminate before use
- Drawbacks:
  - TTL values play big roles and dictate transfer "speed"
    - De Facto Standard for TLD's is 1 day.
  - Old and new DNS operators must cooperate

DNS data flow



DNSSEC transfers:

- For DNS and DNSSEC transfers to work smoothly DNS operator change and Registrar change MUST take place at different times.

Registrar DNSSEC Participation

- Accept DS record via Registrant interface
  - Creation of first one
  - Add
  - Removal
  - Delete of all records

DNS operator Role

- Be able to turn on and OFF DNSSEC
- Be able to accept external DNSKEY records
- Allow update of NS records to external servers.
  - Do not to turn off service when this happens.
- Turn off service when requested
- Zone file view

Import/Export of public key

Must support the import of a public key created by a third party

– Must always be published in the domain's zone, which will be at the registrar if DNS services are bundled with registration services, otherwise at the DNS operator

– Must optionally be published in the parent's zone; "on deck" keys will not be published in the parent zone

Must support the export of a public key created locally

– Gaining DNS operators need their new key information published in the zone file of the Losing DNS operator as an "on deck" key

Import of NS records

- When DNS services are being transferred the registrar must import and publish to the registry the new NS resource record glue set
- Most registrars already do this except that by importing a third party set of NS resource records results in DNS services being discontinued, if the registrar is providing both DNS services and registration services;
  - **this must not happen**